

EC-2000-007
II-A-013

In-house Test Results¹

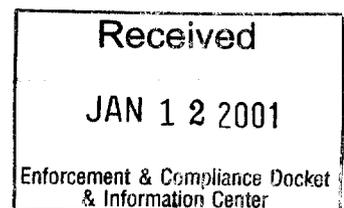
Web-based Submission of the Discharge Monitoring Report ₂

EPA Contract #68-W5-0030³

Delivery Order #0004

Revised August 30, 1999

1	Scope	4
2	Discussion of Specific Test Results	4
2.1	Interaction of Adobe Acrobat Exchange with Web Browsers	4
2.2	Interaction of Adobe Acrobat Exchange with HAHTsite	5
2.2.1	Duplicate Application Server Processes when Saving Form Data	5
2.2.2	Failure to Load Pre-populated Form Data from the Application Server	6
2.3	Interaction of E-Lock Signature Plug-in with Adobe Acrobat Exchange	6
2.3.1	Form Data not Visible with Signature Icon Present under NT	6
2.3.2	Electronic Form Screen Colors Change when Signature Plug-in is Activated	6
2.3.3	Non-standard Screen Cursor Disappears when Signature Plug-in is Activated.	6
2.3.4	Adobe Forms Author Plug-in Required for Signature Verification	7
2.3.5	Memory Overwrite Occurs if Signature Hash is Base64 Encoded	7
2.4	Interaction of E-Lock Signature Plug-in with Cryptographic	



Features of the Windows Operating System	7
2.4.1 CryptoAPI Does Not Close Certificate Store	7
2.4.2 Possible Bypass of Smart Card to Generate Private Key	8
2.4.3 Re-registering Certificate Needed to Reset Cryptographic Service	8
2.5 Interaction of Graphics Tablet Software with the Windows Operating System	8
2.5.1 Problem Restarting Windows 95 after Installation of the Graphics Tablet	8
2.5.2 Lock-up of User Interface When Graphics Tablet is Present	8
2.6 Serial Port Conflicts	9
2.6.1 Serial Port Conflicts Between Smart Card Reader and Graphics Tablet	9
2.6.2 Interference with Modem Connection with Graphics Tablet Installed	9
2.7 Access to the Certificate Authority Server	9
2.7.1 CA Server Cannot be Reached During Registration	9
2.7.2 Enrollment Fails if User Enrolls with Duplicate Information	9
3 In-house Test Results Related to E-Lock Components	10
3.1 Introduction	11
3.2 Certificate Authority for the EPA DMR Project	11
3.2.1 Problems During Registration Process	11
3.2.2 PKI Registration through Firewalls	11
3.2.3 Input Character Problems in PKI Registration Forms	12
3.2.4 Web Browser Independence in PKI Registration Forms	12
3.2.5 Web-based Registration	12
3.3 Digitally Signed Adobe Acrobat Forms for the EPA DMR Project	12
3.3.1 Signature Verification Problem	12
3.3.2 Memory Overrun Problem	13

3.3.3	Adobe Acrobat Form Author Plug-in	13
4	E-mail Messages Related to In-house Test Results	15
4.1	Discussion of the Position of the Window Opened by the Adobe Acrobat Exchange Application and a Problem with Form Colors when Signature Plug-in is Activated	15
4.2	Results of Preliminary Tests of the Local Registration Authority Administrative Console	17
4.3	Results of Tests Conducted at the New York State Department of Environmental Conservation	18
4.4	Digital Signature Verification Issues	20
4.5	Forcing the use of the Smart Card to Generate the Private Signing Key	25
4.6	Problem Simultaneously Connecting a Smart Card Reader and a Graphics Tablet when Only One Serial Port is Available	30
4.7	Status of Support for Adobe Acrobat Exchange 4.0 in HAHTsite	34
4.8	Multiple Adobe Form Windows in Internet Explorer and Duplicate Record Insertion when Storing Form Data using HAHTsite Programming	35

1 Scope

This document describes the results of in-house testing in preparation for 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. The technical issues described in this document are limited to those identified before the pilot hardware and software components were installed on the pilot participant's computers beginning in June of 1999. Technical issues identified after the involvement of the pilot participants are discussed in a separate document entitled, "Technical Issues in Phase 1".

2 Discussion of Specific Test Results

The in-house testing period revealed problems and issues related to the

compatibility and interaction of the principal hardware and software commercial off-the-shelf components as they were configured to meet the requirements of the DMR pilot. Appendix A discusses the experience of E-Lock Technologies with this integration process as it relates to the creation and verification of cryptographic digital signatures within the context of the DMR pilot, as well as issues encountered implementing the public key infrastructure (PKI) environment for the pilot. Some of the test results reported in Appendix A extend into the June, 1999, time period when the pilot participants began to enroll and register with the certificate authority during Phase 1 of the DMR pilot, but are included together with the in-house test results to maintain the context and integrity of E-Lock's "lessons learned" report.

Appendix B contains examples of E-mail messages which reveal vignettes of some of the experience and discussion which occurred during the in-house testing period.

Specific in-house test results are grouped by category in the subsections below.

2.1 *Interaction of Adobe Acrobat Exchange with Web Browsers*

Early in the in-house testing period, it became clear that the Adobe Acrobat Exchange Version 3.01 electronic form behaved differently as a plug-in to the Microsoft Internet Explorer Version 4.01 Web browser compared with the Netscape Navigator Version 4.51 Web browser. When Adobe Acrobat Exchange Version 3.01 was used with Microsoft Internet Explorer Version 4.01, a new browser window opened each time the HAHTsite application server sent a form data type to the browser which would cause the browser to launch Adobe Acrobat Exchange and open a window displaying the electronic form. Since Adobe Acrobat Exchange is a single-threaded application, Adobe Acrobat Exchange would not function correctly with respect to exchanging Form Data Format (FDF) data streams with the application server for any instance beyond the first.

When Adobe Acrobat Exchange Version 3.01 was used as a plug-in to Netscape Navigator 4.51, however, at most one browser window remained opened at any one time no matter how many times the display of an electronic form was triggered by a form data type sent to the browser from the application server.

Preliminary testing revealed that the use of Adobe Acrobat Exchange Version 4.0 as a plug-in to Internet Explorer Version 4.01 did not result in the opening of multiple windows. However, an upgrade to Adobe Acrobat Exchange Version 4.0 was not considered feasible for the pilot because, at the time the in-house tests were conducted, this version was new and its compatibility with versions of the cryptographic and biometric digital signature plug-ins could not be assured. Also, the available version of the HAHTsite application server had not been fully tested with Adobe Acrobat Exchange Version 4.0. A preliminary test of the compatibility of the E-Lock cryptographic digital signature plug-in with Adobe Acrobat

Exchange Version 4.0 revealed that the digital signature plug-in required modification to work with Adobe Acrobat Exchange Version 4.0.

2.2 Interaction of Adobe Acrobat Exchange with HAHTsite

Two issues were observed related to the interaction of the electronic form environment, Adobe Acrobat Exchange Version 3.01, with the application server, HAHTsite Version 3.1.

2.2.1 Duplicate Application Server Processes when Saving Form Data

The design of the electronic form for the DMR pilot required that the electronic form be structured with multiple pages, but be processed as one form when exchanging data with the application server. This required a modification in the default assumption made in the design of the application server as an off-the-shelf product, in which one form page was both displayed and processed as a single unit. When this modification was made, in-house tests showed that the application server created two duplicate instances of the server-side software processes used to store the form data in the database, resulting in duplicate data base records when form data was submitted to the application server. It was necessary to add custom programming to stop one of these duplicate processes each time the application server saved form data to the database.

2.2.2 Failure to Load Pre-populated Form Data from the Application Server

Tests showed that the data needed to pre-populate longer (multiple page) Adobe Acrobat Exchange forms sometimes did not fully load from the application server, resulting in form templates without default data. This behavior was found to be dependent on the size of the public memory cache in the application server.

2.3 Interaction of E-Lock Signature Plug-in with Adobe Acrobat Exchange

The following problems were observed related to the interaction of the E-Lock cryptographic digital signature plug-in, Assured Transactions Version 2.1, with the electronic form environment, Adobe Acrobat Exchange Version 3.01.

2.3.1 Form Data not Visible with Signature Icon Present under NT

When early versions of the E-Lock cryptographic digital signature plug-in were used with Adobe Acrobat Exchange Version 3.01, form data could not be seen on the same page of the electronic form that contained the signature icon if Windows NT was the client computer operating system. A modification of the digital signature plug-in to be compatible with Windows NT was required.

2.3.2 Electronic Form Screen Colors Change when Signature Plug-in is Activated

Tests showed that, on computers with certain screen resolution and color density settings, the color of the Adobe Acrobat Exchange Version 3.01 form would change when the E-Lock cryptographic digital signature plug-in was activated. This problem was mitigated by changing the graphic resolution of the signature icon installed in the electronic form. However a color change continued to be observed in some cases if the client computer's display was set to 256 colors.

2.3.3 Non-standard Screen Cursor Disappears when Signature Plug-in is Activated.

If the shape of screen cursor of the client computer had been changed to a setting other than the default, the cursor would sometimes become invisible when the E-Lock cryptographic plug-in was activated. This problem was not solved, but if the user clicks the mouse outside of the window opened when the signature plug-in is activated, the cursor reappears.

2.3.4 Adobe Forms Author Plug-in Required for Signature Verification

Cryptographic digital signatures created on Windows 95 client computers sometimes could not be verified by the server-side signature verification component. It was discovered that the Adobe Forms Author plug-in was required to be installed on these computers in addition to Adobe Acrobat Exchange, and that the Adobe Forms Fill-in plug-in could not be present. The client-side E-Lock install program was modified to detect the presence of the Adobe Forms Author plug-in and to detect the absence of the Adobe Forms Fill-in plug-in.

2.3.5 Memory Overwrite Occurs if Signature Hash is Base64 Encoded

A memory overwrite (overrun) condition was detected within the Adobe Acrobat Exchange application if the E-Lock digital signature plug-in stored the digital signature hash value in a hidden field of the form in Base64 encoded format. The conversion of a binary digital signature hash value to Base64 encoded format often resulted in the presence of the carriage return and line feed characters in the converted digital signature hash. The Adobe Acrobat Exchange application processed these characters in a special way, causing a memory overwrite to occur within the Adobe Acrobat Exchange application. This memory overwrite caused the client computer to hang or report intermittent "blue screen" or "Dr. Watson" errors. Digital signature verification sometimes failed for this reason. To solve this problem, carriage return and line feed characters were substituted for other characters in the Base64 encoded format when stored in a field of the Adobe Acrobat Exchange form, and then translated back to carriage

return and line feed when received by the application server.

2.4 *Interaction of E-Lock Signature Plug-in with Cryptographic Features of the Windows Operating System*

The following issues were identified related to the interaction of the E-Lock digital signature plug-in with the cryptographic features of the Windows operating system.

2.4.1 *CryptoAPI Does Not Close Certificate Store*

A high-level function within the set of possible Microsoft Cryptographic Application Programming Interface (CryptoAPI) calls does not close the Certificate Store after this CryptoAPI is used by the server-side E-Lock cryptographic digital signature verification component. This resulted in server crashes and failure to verify the digital signatures. This problem was solved by accessing the Certificate Store using a lower-level CryptoAPI call.

2.4.2 *Possible Bypass of Smart Card to Generate Private Key*

Tests of early versions of the E-Lock cryptographic digital signature plug-in showed that the signer could bypass the smart card when signing by selecting a software-based cryptographic service provider to generate the private cryptographic key used by the signature algorithm. The cryptographic digital signature plug-in was modified to require the signer to use the cryptographic service provider supplied with the smart card.

2.4.3 *Re-registering Certificate Needed to Reset Cryptographic Service*

Tests showed that it was occasionally necessary to reset the cryptographic service by re-registering a new certificate with the certificate authority. The conditions which resulted in the need to reset the cryptographic service were not identified.

2.5 *Interaction of Graphics Tablet Software with the Windows Operating System*

The following problems were identified related to the interaction of the graphics tablet (CalComp UltraSlate) used to capture a biometric handwritten signature and its associated software (TableWorks 5.0) with the Windows operating system.

2.5.1 *Problem Restarting Windows 95 after Installation of the Graphics*

Tablet.

On one laptop computer (an IBM ThinkPad 770 running Windows 95), the installation of the CalComp UltraSlate graphics tablet and its associated TableWorks 5.0 software prevented the Windows 95 operating system from starting. It was necessary to remove selected dynamic link library (DLL) files added to the system directory by the graphics table installation to restore the ability of the laptop to boot up under Windows 95. This behavior was not observed on other computers during the testing period.

2.5.2 Lock-up of User Interface When Graphics Tablet is Present

On one laptop computer (an IBM ThinkPad 770 running Windows NT), the keyboard and mouse locked up (would not function) if the graphics tablet was connected to the serial port of the computer. On other computers, a lockup of the user interface occurred if the graphics tablet was not firmly plugged into the serial port.

2.6 *Serial Port Conflicts*

The following test results were observed and believed to result from a conflict of two software drivers for the same serial port.

2.6.1 Serial Port Conflicts Between Smart Card Reader and Graphics Tablet

Serial port conflicts were observed if both the Gemplus GemSAFE Version 1.0 software supporting the Gemplus GCR-410 smart card reader and the TableWorks Version 5.0 software supporting the CalComp UltraSlate graphics tablet were installed on the same computer and configured for the same serial port, even though only one device was attached to the serial port at any one time.

2.6.2 Interference with Modem Connection with Graphics Tablet Installed

Interference with dial-up communication using a modem was observed on one computer when the CalComp UltraSlate graphics tablet was connected to the serial port of the computer.

2.7 *Access to the Certificate Authority Server*

The following test results were observed related to the certificate authority server. Additional observations can be found in Appendix A, Section 3.2.

2.7.1 CA Server Cannot be Reached During Registration

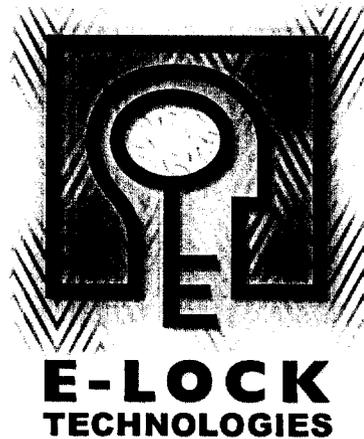
Problems accessing the certificate authority server over the Internet were sometimes observed. During the in-house testing period, these access problems were related to network congestion at or near the certificate authority's site. After the pilot participants became involved in Phase 1, it was discovered that firewalls could prevent access to the certificate authority server, although access through the firewall maintained by the New York State Department of Environmental Conservation was not a problem during the testing period.

2.7.2 Enrollment Fails if User Enrolls with Duplicate Information

Enrollment of identity information with the certificate authority failed if the identity information duplicated exactly previous information which had been enrolled. This problem was addressed by allowing the enrollment to succeed from the viewpoint of the person attempting the enrollment and letting the Local Registration Authority administrator resolve the duplicate identity information.

Appendix A

3 In-house Test Results Related to E-Lock Components



EPA DMR Project

Lessons Learned

Revised August 27, 1999

Introduction

Certificate Authority for the EPA DMR Project

Problems During Registration Process

PKI Registration through Firewalls

Input Character Problems in PKI Registration Forms

Web Browser Independence in PKI Registration Forms

Web-based Registration

Digitally Signed Adobe Acrobat Forms for the EPA DMR Project

Signature Verification Problem

Memory Overrun Problem

Adobe Acrobat Form Author Plug-in

3.1 *Introduction*

This document discusses the lessons learned during the integration and deployment of the E-Lock Technologies PKI and Adobe Acrobat form signing products and services for the EPA DMR Pilot. This document contains two sections, one that describes the lesson learned with the Certificate Authority deployment and one section that describes the lessons learned from the Adobe Acrobat form signing deployment.

3.2 *Certificate Authority for the EPA DMR Project*

This section discusses the lessons learned with the deployment of the EPA Certificate Authority.

3.2.1 **Problems During Registration Process**

A number of times the error codes 80048001 and 80048002 were reported during the Registration process with the e-Lock PKI Server. These error codes are returned in the case where the e-Lock PKI Client application is unable to establish a connection with the e-Lock PKI Server. This could be due to a possible configuration problem (i.e., incorrect IP or host specification or registration server access point). These errors could also be presented due to temporary unavailability of the e-Lock PKI server either due to intermediate network failure or genuine unavailability of the PKI server due to scheduled maintenance activity.

3.2.2 **PKI Registration through Firewalls**

Accessing PKI Server through firewall environments. This had been an issue with some participant companies that prevented them from using the "Register with PkiServer" application since the application was not designed to be configured to re-route its traffic through firewall proxy server. However this issue has been resolved by providing a browser based certificate enrollment procedure. The EPA CA LRA Administrator console would incorrectly report duplicate users while adding user records that are distinct from any of the

existing user records. This problem was researched and has been corrected.

3.2.3 Input Character Problems in PKI Registration Forms

EPA certificates were showing some subject fields as non-printable character strings. The cause was determined to be a Microsoft Certificate Server limitation. The problem would result from the input of a certificate request which contained some disallowed characters like '_' or '#'. This limitation was researched and the user interface was updated to restrict input of these characters.

3.2.4 Web Browser Independence in PKI Registration Forms

The Reporting Company registration and enrollment page, where the user is expected to provide information that appears in the digital certificate issued by the EPA CA, was not originally designed to work with Netscape Communicator web browser. This problem was researched and support was added for the Netscape Communicator web browser. However the EPA CA LRA administration console continues to remain specific to the Microsoft IE 4.0 or higher web browser and does not support the Netscape Communicator web browser. One of the pre-requisites for installing the E-Lock Technologies PKI software to support the EPA CA is the Microsoft IE 4.0 or higher web browser so we do not consider this limitation to be a serious shortcoming. Also, the administrator console is restricted to a select few users/administrators, so those that would require the Microsoft IE 4.0 web browser would be small.

3.2.5 Web-based Registration

Some of the EPA reporting companies reported problems trying to use the e-Lock PKI client installed with e-Lock EPA Client install. These problems generally related to restrictions placed on network traffic by the Reporting Company's firewall. To solve this problem, E-Lock Technologies supplied a fully web-based alternative registration method to the e-Lock PKI Client.

3.3 Digitally Signed Adobe Acrobat Forms for the EPA DMR Project

This section discusses the lessons learned during the deployment of the digitally signed Adobe Acrobat forms.

3.3.1 Signature Verification Problem

The e-Lock ATS Adobe Acrobat signature verification control had a problem with the usage of Microsoft CryptoAPI DLL. The symptoms were those of a memory leak, but the problem was that a CryptoAPI Certificate Store was left open after use. The problem was corrected in the e-Lock ATS Adobe Acrobat signature

verification control and this problem was fixed.

3.3.2 Memory Overrun Problem

After filling the Adobe Acrobat form with data and clicking the Submit button in the context of the browser, a "Cannot read Memory: Page Fault" error was occurring. This problem was thoroughly researched and debugged and it was found that the problem was due to a memory-overrun problem in the Adobe Acrobat AFORM32 module.

The following is a short technical explanation of the problem. The e-Lock ATS digital signature string is BASE64 encoded to allow it to be sent on any underlying transport implementation. The BASE64 encoding contains the characters 0x0D and 0x0A (in hexadecimal notation). A routine in the AFORM32 plug-in was parsing the digital signature string and while doing this it was looking for characters 0x0d, 0x0a and 0x20 (space). If it encounters these characters it would treat the data differently. It was determined that in the case where the 0x0d character was found by the AFORMS plug-in, the counter for the signature buffer wasn't getting incremented but the signature buffer pointer was getting incremented. This resulted in an overrun of the signature buffer each time (i.e., each time the form was submitted). The crash condition was coming when this signature buffer was on a memory page boundary where the overrun resulted in a page-fault.

The problem was corrected by replacing the character 0x0d with 0x80 and the character 0x0a with 0x81. These characters would not normally occur in a BASE64 encoded data stream, so upon receiving this data stream at the server the e-Lock ATS server replaces the original characters back into the BASE64 encoded data stream (i.e., 0x0d and 0x0a). This same solution also helped in another AFORM32 plug-in problem where at times, extra bytes were sent by the AFORMS32 plug-in as part of the signature data (as a result of the 0x0d and 0x0a characters being present), which caused the signature verification to fail.

3.3.3 Adobe Acrobat Form Author Plug-in

There was a problem with the Adobe Reader form fill-in plug-in vs. the Adobe Form Author plug-in.

The product was using the fill-in plug-in (fillerus.exe) when problems were experienced with Signature verification. After some research, it was found that removing the Acrobat Fill-in Plug-in and using the Acrobat Forms Author Plug-in solved this problem. A review of the Adobe web site for the usage of these plug-in revealed the following information.

Excerpt from Adobe Acrobat Forms Author Plug-in

The Adobe Acrobat Forms Author plug-in 3.5 adds new features to PDF forms you create and view in Adobe Acrobat Exchange 3.01. The Acrobat Forms Fill-in plug-in 3.5, which you use in Acrobat Reader rather than Acrobat Exchange, lets you view PDF forms containing new features created with the Author plug-in.

NOTE: Don't install the Fill-in plug-in if you're using Acrobat Exchange -- the Fill-in plug-in is designed only for Acrobat Reader. Acrobat Exchange's form tools will be unavailable if you install the Fill-in plug-in.

The Author plug-in requires Windows 95, Windows NT 3.5.1 or later (it will not run in Windows 3.1x), or Apple System Software 7.1 or later. The Fill-in plug-in requires Windows 95, Windows NT 3.5.1 or later, Windows 3.1x, Apple System Software 7.1 or later, HP-UX, IBM-AIX, SunOS, or Sun Solaris.

Switching to the use of Adobe Acrobat Forms Author plug-in solved the problems experienced with signature verification failures.

Appendix B

4 E-mail Messages Related to In-house Test Results

The following E-mail messages are related to some of the issues identified during in-house testing. These example messages provide a window into the nature and detail of some of the discussions related to these tests within a time snapshot defined by the scope of the individual E-mail messages. These messages do not track any given issue from conception to resolution.

4.1 *Discussion of the Position of the Window Opened by the Adobe Acrobat Exchange Application and a Problem with Form Colors when Signature Plug-in is Activated*

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

From: Lewis, Todd
Sent: Thursday, May 27, 1999 12:03 PM
To: 'Steve Vogler'
Cc: cshaugh@gw.dec.state.ny.us; 'IDI-EPA Distribution';
'Kimberly Nelson'
Subject: RE: Installation of new E-LOCK (initial NYS DEC results)

Steve, thank you for doing this test, and of course I'm happy to hear that you were successful in submitting a DMR form from New York! The fact that the Adobe Exchange window pops up in front of your browser window is something that we have noticed, but there may not be a solution for this annoyance, since the placement of a window when an application launches is probably outside the control of any coding within the DMR form, and also outside the control of coding which exists on the server. There may be a way to automatically minimize the Adobe Exchange application, but this doesn't seem likely from a theoretical perspective. However, I'll check to see if there is a trick we don't know about yet.

I believe the multiple colors you observe in the DMR form are the result of a temporary mismatch in resolution and color density between those used in the form and/or an icon on the form (such as the E-Lock signature icon) and the current resolution and color density you have configured for the graphics card you are using in your computer. When you

begin to enter data, the form is repainted and the initial mismatch disappears. There may be a way to force a repaint when the form is loaded. Whether this can be done depends upon the functionality available for setting such a command within the Adobe representation of the DMR form. Again, this is asking for coding within the Adobe Exchange form to trigger an event within the Adobe Exchange plug-in on your computer before you interact with the form in any way. I'm not sure this is possible within the scope of the Adobe product, but I'll check on this point as well.

Thank you,

Todd
TLewis@idinc.com

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

From: Steve Vogler [<mailto:sevogler@gw.dec.state.ny.us>]
Sent: Thursday, May 27, 1999 11:09 AM
To: TLewis@idinc.com
Cc: cshaugh@gw.dec.state.ny.us
Subject: Installation of new E-LOCK

Hi Todd, both the Adobe Form Author and the new E-LOCK installations worked well. I was also able to submit a DMR with the Smart Card Reader signature on it. Two things different that I did observe:

- 1) when I picked a SPDES#, monitoring period and discharge pipe and hit submit the Acrobat Exchange window appears in front of the DMR form. You have to either minimize the Exchange window or click on the DMR form.
- 2) The form appears in multiple colors before I enter any data.

I will be out of the office on Friday but I will try some more testing next week.

Thanks for you help
Steve

4.2 *Results of Preliminary Tests of the Local Registration Authority Administrative Console*

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

From: Lewis, Todd
Sent: Friday, May 07, 1999 8:46 AM
To: 'Jayant Sane'; 'Ray Langford'
Cc: 'IDI-EPA Distribution'; Liu, WeiShing; Yang, AnPing
Subject: Feedback on Local Registration Authority Administrative Console from May 6 Tests

Jayant & Ray, the LRA administrative console (and the enrollment and registration process with the certificate authority server in general) was extremely successful and effective based on the May 6 tests at the New York State Department of Environmental Conservation tests in Albany, New York. The workflow made sense and did allow for the kind of negotiation between the LRA administrator and the certificate requester which is needed. Thank you so much for putting this together quickly. The following points represent feedback from NYS DEC:

- 1) When the LRA administrator updates a certificate request, the requester doesn't receive any indication of what change the LRA administrator is recommending. Since these changes can be subtle (e.g., Information Dynamic vs. Information Dynamics vs. Information Dynamics, Inc. vs. Information Dynamics Inc.) it can be difficult for the requester to understand what change the LRA administrator is proposing. The recommendation would be to include in the E-mail message and/or on the Web page an audit trail of the precise changes the LRA administrator made in the update (e.g., company: original value = Information Dynamic; proposed value = Information Dynamics).
- 2) The Web page referenced by the URL containing a serial number found in the E-mail message provided by the CA server notifying the requester of the proposed updates refers to a Web page at the CA site which does not appear to remain active throughout the process of negotiating the certificate request content (e.g., the Web page goes away too quickly in the process; the Web page should remain active at least until the requester receives his access code).
- 3) When the URL pointing to the CA Web pages is long enough that E-mail client word wrap can break the URL across two lines. If this occurs, the user can't click on the hyperlink in the E-mail message and receive the correct Web page without noting in the body of the E-mail message what didn't get included on a single continuous line and then repairing the URL by typing this extra information at the end of the URL obtained by clicking on the hyperlink or performing a cut and paste operation. The suggestion would be to use a virtual path on the CA server which would allow shorter URLs.
- 4) If two LRA administrators are working at the same time, and a second LRA administrator approves a pending certificate request, then the first LRA administrator receives a low-level database error when attempting to access these pending records.

- 5) The Web form field lengths to capture identity information are too short to contain the data used by NYS DEC. The E-mail field especially is too short.
- 6) The purpose and definition of fields in the default settings option is not clear.
- 7) It would be helpful to have a default option to set the certificate expiration date to an absolute calendar date (e.g., March 31, 2000). All certificates for the EPA DMR pilot will be set to expire at the end of New York State's fiscal year.
- 8) Some Web forms do not display in Netscape Navigator (the browser component of Netscape Communicator 4.51).

Thank you,

Todd
TLewis@idinc.com

4.3 *Results of Tests Conducted at the New York State Department of Environmental Conservation*

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

From: Lewis, Todd
Sent: Friday, May 07, 1999 8:18 AM
To: 'Ray Langford'; 'Manisha Tidke'
Cc: 'IDI-EPA Distribution'; Liu, WeiShing; Yang, AnPing
Subject: Overall Impressions of May 6 Tests at NY DEC

Ray & Manisha, here is my overall impression of the results of the May 6 tests at the New York State Department of Environmental Conservation in Albany, New York. These are feeling-level impressions and are based on test results which were detailed in a previous message.

- 1) The success of the pilot design depends upon keeping the Adobe Acrobat Exchange plug-in to the browser healthy throughout the submission process, since Adobe Acrobat Exchange must mediate the data transfer between the client and the server.
- 2) Test results (e.g., "illegal operation", "Dr. Watson" and "fatal exception" messages on a wide variety of client computers, in addition to screen display changes which don't refresh to normal) provide a clue that the Adobe Acrobat Exchange plug-in to the browser is not being maintained in a healthy state throughout the form signing and submission process. This hypothesis is reinforced by at least one Dr. Watson result which identified the Adobe Exchange as the application reporting the error.

- 3) Since there is evidence that the E-Lock digital signature plug-in to Adobe Exchange seems to trigger error conditions, the two primary logical conclusions are either: a) the E-Lock plug-in damages Adobe Exchange, or b) Adobe Exchange damages the E-Lock plug-in (e.g., by returning a pointer to invalid memory as the result of an API call by the E-Lock plug-in).
- 4) Since the Adobe Exchange plug-in is supported (at least by Haht Software under Netscape Navigator) as a method of transferring data to/from an Adobe user interface and a database at a Web site, there is some reason to believe that the Adobe Exchange form would be stable under at least some defined circumstances. However, it would be worth knowing (perhaps from one of your inside contacts at Adobe) whether more is known about the overall stability of Adobe Exchange 3.01 acting as a browser plug-in, where the specific browsers are Internet Explorer 4.01 SP2 and Netscape Navigator 4.51 (the browser component of Netscape Communicator 4.51) running under Windows 95 and Windows NT 4.0.
- 5) In one test, changing the memory characteristics of Windows 95 (e.g., changing the virtual memory settings) affected the observed behavior of the Adobe Exchange/E-Lock plug-in, suggesting that available memory could be a variable in the observed test results. [It may be worth running a utility which occupies a pre-set amount of RAM memory to see if client problems could be reproduced more efficiently.]
- 6) Since the behavior of the server signature verification is observed to depend on the state of the client, it could be difficult to debug the server application until it is clear what data are being received by the server from the client. This also implies that the client is not behaving as expected across various different client configurations (e.g., Windows 95 vs. NT, Internet Explorer vs. Netscape, amount of available virtual memory, etc.).
- 7) The pilot would fail if implemented without change under the current conditions. The highest priority need is to determine why the browser/Adobe/E-Lock combination is not stable across a variety of computers. The different detailed test results and error conditions is suggestive of a random memory overwrite or some other error which manifests itself in different ways on different client configurations.

Thank you,

Todd
TLewis@idinc.com

4.4 *Digital Signature Verification Issues*

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

From: Lewis, Todd
Sent: Wednesday, May 05, 1999 10:55 PM
To: 'Manisha'; Liu, WeiShing; 'ani'
Cc: idi-epa@elock.com; Yang, AnPing
Subject: RE: Finally the Server Verification succeeded.

Manisha, I received the same error today (in testing) when attempting to submit an Adobe Exchange form which I had just signed with the E-Lock plug-in. It seems that things begin to go wrong when Adobe Exchange is used more than once. WeiShing obtained a preliminary result which seemed to show that the behavior of Adobe Exchange as an Internet Explorer 4.0 plug-in could be made more stable if a "MenuItem File Exit" procedure was added to a "Mouse Up" action linked to the submit button. Outside of the browser plug-in context, this would simply cause Adobe Exchange to exit once the mouse was pressed and then released on the submit button. When Adobe Exchange is used as a plug-in to Internet Explorer 4.0, this "Mouse Up" action didn't cause Adobe Exchange to exit, but it seemed to improve the stability of the Adobe Exchange - IE 4.0 combination if it were reused, suggesting that Adobe Exchange as a plug-in leaves a thread-process-memory allocation open to create problems on reuse. I'm sharing this observation in case part of the solution is finding a way to make sure Adobe Exchange shuts down after a signature is executed. On the server, how are you reconstructing the Adobe Exchange form with data? I would think you would need to run Adobe Exchange on the server for the verification and let the Adobe API report the contents of a reconstructed form as input to the signature verification algorithm. If this is not the case I would be curious how you are obtaining the content of the reconstructed form for this purpose on the server. If it is the case, then perhaps part of the solution for verification could be to make sure that Adobe Exchange shuts down after each verification.

Thank you,

Todd
TLewis@idinc.com

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

From: Manisha [mailto:manisha@fcpl.co.in]
Sent: Wednesday, May 05, 1999 8:27 AM
To: Liu, WeiShing; 'ani'
Cc: idi-epa@elock.com; Lewis, Todd; Yang, AnPing
Subject: Finally the Server Verification succeeded.

Hi Weishing,

I connected to discovery.idinc.com and Signed the form using certificate issued by the epa-ca. And IT VERIFIED the form Signature Successfully and I got the next page : Attached is the bmp of this page. (success.zip)

Then I did the following:
click help->help page.
resubmit.
pdf -resubmit again.

This time I got this error:

HAHTsite 3.1 webapps Server reports the following:
The application had a runtime error while processing this page. Report this problem to the site webmaster along with a copy of the URL that caused this message.

HAHTsite 3.1 webapps Server reports the following Error:
The application had an unhandled error while running page upd_btnSubmit.
Runtime error 900 occurred at line 2939 in
pdffile\upd_naxdmr: A system exception occurred executing
line 2939 in routine upd_naxdmr_ETI_VerifySignature.

We are trying to solve the error you are getting there.

With regards
Manisha.

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

From: Liu, WeiShing <WLiu@idinc.com>
To: 'ani' <ani@fcpl.co.in>
Cc: 'idi-epa@elock.com' <idi-epa@elock.com>; Lewis, Todd <TLewis@idinc.com>;
Yang, AnPing <AYang@idinc.com>; 'manisha@fcpl.co.in' <manisha@fcpl.co.in>
Date: Tuesday, May 04, 1999 11:48 PM
Subject: Server Verification.

>Hi Ani,

>Follow step list by you.

>Successfully installed. However we have some problem still.

>1. Set Adobe Exchange weblink to IE.

>I submitted with a successful result.

Since I did not sign penop. NoFrames page been brought up.
click help->help page.

resubmit.

pdf -resubmit again. I received two different errors with
several tries.

>FIRST. <<first.ZIP>>

>second. <<fail1.ZIP> <<fail2.ZIP>>

>2. Set Weblink to Netscape.

>I received first.zip error when I try to submit it. (with
E-Lock check mark)

>I tried several times, increased HAHTsite public space from
512K to 2MB. same result.

>conclusion: It will be successful the first time (weblink
link to ie) failed after. No luck for Netscape at all
(always failed).

>log file attached.

<<hahtsrv.log>>

>Thank You.

>Weishing Liu.

>-----Original Message-----

>From: ani [SMTP:ani@fcpl.co.in]

>Sent: Tuesday, May 04, 1999 12:01 PM

>To: Liu, WeiShing; 'Manisha'

>Cc: idi-epa@elock.com; Lewis, Todd; Yang, AnPing

>Subject: Re: Forgot to mention..

>

>Liu,

>

>I think there is some configuration problem on your

discovery machine which is causing this problem. Just to make sure that we have not missed any steps, can you do the following:

- >
- >1. Open Regedit and search for "etipdfverf.dll". Wherever you find this,
 - >delete the key and the container (the node in which it is defined -- it looks like guid).
- >2. After you have done this, uninstall the e-Lock ATS product.
- >3. Delete the directory d:\epa-dmr\elock.
- >4. Restart the machine.
- >5. Install the e-Lock ATS 2.1 with options for Adobe form signing SDK, e-Sign ActiveX SDK and the e-Sign application.
- >6. Copy the attached latest etipdfverf.dll file in the "<install directory>\Adobe Acrobat Form Sign SDK" directory. Make sure before copying that the installation had put the etipdfverf.dll in that directory.
- >7. Register fdfacx.dll from the above directory.
- >8. Register etipdfverf.dll from the above directory.
- >9. Publish your "current" project once again.

>

>Now try the Adobe form signing and verification. Please send us a mail about what happens. Also, ring up Manisha to inform her of the same if it is not later than 2pm your time. She can be reached at:

>

>91-20-5670064

>

>

>Thanks

>

>Ani

>

>----- Original Message -----

>From: Liu, WeiShing <WLiu@idinc.com>

>To: 'Manisha' <manisha@fcpl.co.in>

>Cc: <idi-epa@elock.com>; Lewis, Todd <TLewis@idinc.com>; Yang, AnPing <AYang@idinc.com>

>Sent: Tuesday, May 04, 1999 8:46 PM

>Subject: RE: Forgot to mention..

>

>

>Hi Manisha,

>

>I tried to regsvr32 /u etipdfverf.dll. failed. with 0xc0000005 code.

```
>
>ignore error. continue steps.
>
>fdfacx.dll and etipdfverf.dll point to same place. under
>c:\program files\elock-1\elock ats\abode....
>
>I received same error message. No log file generated.
>search c and d drive.
>
>Weishing Liu.
>
>
>-----Original Message-----
>From: Manisha [SMTP:manisha@fcpl.co.in]
>Sent: Tuesday, May 04, 1999 10:49 AM
>To: WeiShing Liu
>Subject: Forgot to mention..
>
>Hi ,
>
>I forgot to mention:
>After you successfully register the fdfacx.dll and the
etipdfverf.dll from the c:\program files\elock-1\elock
ATS\Adobe directory, Goto the Services icon in the control
panel again. Then
>Start the ftp. smtp, www, services again which would
automatically start the IIS ADMIN Service and then you can
try the demo again.
>
>
>Manisha Tidke ( manisha@fcpl.co.in <
mailto:manisha@fcpl.co.in)
>*****
>To provide security middleware integrating PKI & VPN into
business processes to implement high value Assured
Transactions.
>
>Visit our website at WWW.Elock.Com <http://www.Elock.Com>
>*****
><< File: ETIPDFVERF.dll >>
```

4.5 *Forcing the use of the Smart Card to Generate the Private Signing Key*

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

From: Lewis, Todd
Sent: Monday, May 03, 1999 10:37 AM
To: 'Ray Langford'; 'Manisha Tidke'
Cc: 'IDI-EPA Distribution'; Liu, WeiShing; Yang, AnPing;
'Allen Klumpp'
Subject: RE: E-Lock Adobe Plug-in will execute and store
signature even
if smart card is not in smart card reader

Ray, at least one of these two tests (of signing an Adobe Acrobat Exchange PDF form with the smart card not present) was done using a fresh client laptop at the EPA (on which the pilot software had not been installed) and then using all of the standard install shields for the browser software, Adobe Acrobat Exchange software, GemPlus software, and E-Lock client software. The use of the E-Lock install software in the version we currently have did not result in a configuration in which the GemPlus CSP was automatically selected over the Microsoft base CSP or the Microsoft advanced CSP. This selection was still a manual selection by the end user.

Regarding the tests today, please page me at 1-888-929-7937 to discuss setup for the tests when you are ready.

Manisha, Nilambari and WeiShing worked Friday, Saturday and Sunday on attempting to demonstrate server-side signature verification on the pilot production server but were unsuccessful. At this point, unless you have a better idea, I think we need someone from E-Lock to see the configuration of the pilot production server at 400 Virginia Ave., SW, Suite 110, Washington, DC 20024-2730, and to experience the behavior of the E-Lock server-side software first hand. There doesn't seem to be evidence that the E-Lock etiverfpdf.dll software component is being triggered. What is your suggestion to resolve this?

Thank you,

Todd
TLewis@idinc.com

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

From: Ray Langford [<mailto:ray@elock.com>]
Sent: Friday, April 30, 1999 6:43 PM
To: Lewis, Todd; 'Manisha Tidke'
Cc: 'IDI-EPA Distribution'; Liu, WeiShing; Yang, AnPing

Subject: Re: E-Lock Adobe Plug-in will execute and store signature even if smart card is not in smart card reader

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

From: Lewis, Todd <TLewis@idinc.com>
To: 'Manisha Tidke' <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>
Date: Friday, April 30, 1999 1:59 PM
Subject: E-Lock Adobe Plug-in will execute and store signature even if smart card is not in smart card reader

Manisha or Ray, in a test I did today on one of EPA's laptops (part of the in-house testing for the EPA DMR Pilot), it was clear that the E-Lock Adobe Plug-in we currently have will successfully execute a signature on the Adobe Exchange form and store the signature hash in the Adobe Exchange form field designated for this purpose even if no smart card is inserted into the GemPlus smart card reader. Later today WeiShing and I repeated this test with a different GemPlus smart card reader using the certificate which WeiShing obtained today from E-Lock. Clearly, in two separate tests, the presence of the smart card in the smart card reader was not essential for the E-Lock plug-in to execute the chosen cryptographic algorithm and store the result in the Adobe form field established for this purpose. We were able to confirm that the signature hash was sent as part of the FDF data stream from the client to the server and could be found in the database (SQL Server) under the condition that no smart card was present in the GemPlus smart card reader.

I presume that this could occur because the E-Lock plug-in received the required private key upon a call to the Microsoft Cryptographic API. Clearly, however, this is not the desired result, since the signature should not be successful in the absence of the smart card. Would you please help us understand what is really going on here? Obviously the GemPlus smart card reader is providing information to the Microsoft Cryptographic Service Provider and the E-Lock plug-in is using CAPI calls to communicate with the Microsoft CSP. However the overall result is not what is required. There has to be either a setting in the GemPlus software to prevent the Microsoft CSP from releasing the private key to the E-Lock plug-in if there is no smart

card in the smart card reader, or there has to be a way for the E-Lock plug-in to query the Microsoft CSP to, in turn, query the GemPlus software to determine the presence of a smart card in the smart card reader. In any case, the current observed behavior doesn't meet the fundamental requirement that the execution of a signature require the presence of the smart card.

What light can you shed on this observation?

→ I think what you saw was the following. For testing purposes, WeiShing generated a keypair in the Microsoft base CSP (private key stored in software) and Jayant issued an EPA certificate to this public key. Separately, a different keypair was created on the GemPlus smartcard (private key stored on smartcard) and Jayant issued a certificate to that public key. There is no private key sharing between CSPs. When you performed the two signing operations, you used the two different keypairs (different private keys from different CSPs) and both had certificates issued by the EPA CA. In the context of the EPA pilot, keypairs will only be generated in the context of the GemPlus smartcard and CSP. The EPA Client install will install and preconfigure the e-Lock PKI client to only generate keypairs on the GemPlus smartcard as part of the user entering their PIN provided by the EPA Administrator.

→ If someone were to sign a form with a keypair that had a certificate issued from a different CA, the verification would fail when they submitted the form because the form verification will only succeed if with keypair used to sign had a certificate issued by the EPA CA.

→ Please let me know if you have further questions/concerns on this issue.

Also, on a tangentially related subject, when will a new version of the E-Lock client plug-in be available? [I leave for New York on Tuesday afternoon, May 4.] Known problems in the current E-Lock Adobe plug-in as the result of our in-house testing include:

- 1) Instability (crash) if a signature is attempted when smart card is not fully inserted or a signature hash pre-exists in the Adobe Exchange form field established for this purpose.

→ We are currently testing with the GemPlus smartcard to reproduce this problem in the Mequon office.

2) Interference with the display of Adobe form field formats and data in a full-size window under NT 4.0 SP4.

→ Manisha would need to comment on the status of this problem.

Also, when I am in New York (May 5 - 7) I will need to be able to demonstrate the mechanism for pilot participants to enter identity information at the E-Lock Web site and for the New York State Department of Environmental Conservation to review the entries and approve the identity information. The New York State Department of Environmental Conservation participants in the pilot will also need to be able to establish certificates for their own in-house testing purposes.

→ We are in the process of testing two installables. The EPA Client install, which Al had previously sent, and the EPA Administrator install. The EPA Administrator install will put the necessary PKI Client components on the computer and similar to the EPA Client install, preconfigure for the EPA CA and the GemPlus smartcard.

→ As I mentioned previously, on Monday, May 3, we would like to have a "live test run" with you. Monday morning, we will put the latest EPA Client and EPA Administrator installs for download. On Monday evening, we will send you a CDROM for Tuesday am delivery which contains the EPA Client install and the EPA Administrator install.

→ You would need to setup two computers with GemPlus smartcards, one will be the "EPA Client", the other will be the "EPA Administrator".

→ EPA Client:

- 1) Install E-Lock EPA Client software
- 2) Connect to EPA CA enrollment website, fill out and submit enrollment form.
- 3) After EPA Administrator approves certificate request, an

email will be sent with PIN.

4) Upon receiving the email with PIN, run "Register with PKI Server" and enter PIN to generate signature keypair on GemPlus smartcard and receive certificate from EPA CA.

5) Use keypair on GemPlus smartcard with EPA certificate to sign Adobe Acrobat DMR form.

→ EPA Administrator

1) Install E-Lock EPA Administrator software.

2) Receive PIN from EPA CA Administrator (Jayant).

3) Run "Register with PKI Server" and enter PIN to generate web client authentication keypair on GemPlus smartcard and receive certificate from EPA CA.

4) Connect to EPA Administrator web pages (authenticated via GemPlus smartcard) to approve/disapprove certificate requests from EPA Clients.

→ We should plan a time on Monday (after 10:00am CDT) to teleconference during this "live test run" to work out any final problems/concerns.

For the roll-out of the pilot to the seven participating companies on May 24, it would be desirable to provide them with as an "off-the-shelf-looking" copy of the E-Lock client product as possible. Is there any chance that the final install could be placed on an E-Lock Install CD for this purpose?

→ After the "live test run" and comments during the period between May 5 and May 24, we plan to update the current installs as necessary and send a new CDROM.

→ Please let us know if you have any comments/questions.

→ Thank you.

→ Ray

Thank you,

Todd

>TLewis@idinc.com

4.6 *Problem Simultaneously Connecting a Smart Card Reader and a Graphics Tablet when Only One Serial Port is Available*

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

From: Lewis, Todd
Sent: Wednesday, April 28, 1999 2:13 PM
To: 'Kimberly Nelson'
Cc: 'Victoria Cooper'; 'Mark Weaver'
Subject: FW: GCR420 Support PS/2 Information Dynamics/ Todd Lewis

Kim, here is the response from GemPlus on smart card readers which would not take up a serial port. As you can see, GemPlus is not willing to release, for the purposes of the EPA DMR pilot, the current version of their reader which connects between the PS/2 keyboard port of a computer and a keyboard due to the existence of too many nonstandard keyboards on the open market. Although the E-mail from Mark Weaver (see below) doesn't explicitly say so, it seems that GemPlus is concerned about the support or liability issues (???) that their current recalled PS/2-Keyboard reader (Model GCR420) could generate even in a pilot with 20 users and a supplied compatible keyboard. The GemPlus recommendation is to use their PCMCIA reader, which would work in laptops with a free PCMCIA slot, or in desktops if a PCMCIA Converter (e.g., <http://www.technobox.com/pic1473.htm> and <http://www.technobox.com/cat1473.pdf>) were installed.

We have tested the simultaneous connection of the GemPlus smart card reader which uses a PS/2 keyboard port and a DB-9 serial port (Model GCR410) with the CalComp graphics tablet (which uses a PS/2 mouse port and a DB-9 serial port) in a Windows 95 desktop machine which has two available serial ports, a PS/2 mouse port and a PS/2 keyboard port. This combination works but of course the desktop must have all the required available ports (which not every desktop in the pilot would have).

Given the GemPlus response, the only way to have both a smart card reader and the graphics tablet simultaneously installed would be to use the PS/2-Serial (GemPlus Model GCR410) smart card reader in desktops which have (in addition to the PS/2 keyboard port and DB-9 serial port required by the smart card reader) a PS/2 mouse port and a

second functioning and available serial port. For those desktops which do not have the required ports then the options are: 1) add the required ports to the desktop, or, 2) install a PCMCIA Converter in the desktop so that the GemPlus PCMCIA smart card reader could be used.

In either case this would involve highly technical support to the pilot participants to help them modify and test their computers. A possible "fall back" position would be to identify the subset of pilot computers which could accept both the PS/2-Serial (GemPlus Model GCR410) smart card reader and the CalComp graphics tablet (i.e., those computers which have a PS/2 keyboard port, a PS/2 mouse port and two available, functioning DB-9 serial ports) and use these computers for a test of a simultaneous cryptographic and biometric signatures. The remainder of the computers could be used for the biometric signature alone. This would work only if there were at least one computer at each pilot site which could be used for simultaneous cryptographic and biometric signatures. If not, then a computer for this purpose would need to either be configured with extra hardware or provided.

What are your thoughts on this issue?

Thank you,

Todd
TLewis@idinc.com

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

From: Mark.Weaver@gemplus.com [mailto:Mark.Weaver@gemplus.com]
Sent: Wednesday, April 28, 1999 6:26 AM
To: tlewis@idinc.com
Cc: Victoria.Cooper@gemplus.com
Subject: GCR420 Support PS/2 Information Dynamics/ Todd Lewis

Hello Todd,

I was conferring with Victoria Cooper yesterday regarding this issue for you. Currently, the GCR420 has been removed from our available readers for sale. There are some issues being addressed relating to hardware and software of this reader and assorted computer manufacturers. We are not selling this reader until the New Release of the GCR420 in

the Fall (Q4). We can not send you a GCR420 Reader cause the Pilot that you are going to development will not be compatible with the New GCR420.

What we recommend. We can suggest that Gemplus also offers a PCMCIA Reader to interface with Laptops. It is the GPR400 Reader. This reader can also be used in a desktop machine however, you would have to purchase from a computer store PCMCIA Convertor to install in a vacant drive door to utilize this reader, if this is an option.

If not, then the Marketed GCR420 Reader will not be available until Q4 Fall 1999. Once again this is a totally re-engineered reader. We are addressing an issue that Computer Manufactures are having. Their problem is a Non-Standard Keyboard Architecture Guideline. This Non-Standardization has caused problems with our Gemplus GCR420 Reader. Our R & D has determined the fault and has initialized a correction to this. This is a Fantastic technology that Gemplus possesses and it will be once again available shortly. It allows for a very flexible PC Security System.

As it stands now, we currently can not provide a GCR420 PS/2 Reader for your Secured application for the Environmental Protection Agency. We will have one shortly and perhaps the GPR400 and GCR410 are possible solutions for you.

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

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

Recap of your Verbal Question:

Hello Mark,

I received your name from Victoria Cooper. I have some question relating to the GCR420 Reader. Can you assist me? I need to have a reader that is PS/2, which is your GCR420 Reader. I would like to order one for a small pilot program. We can not use a Serial Port cause we would need it available for a Graphics Tablet for Signatures and at the same time use Smart Card Technology. This pilot is for the Environmental Protection Agency. They will be sending compliance reports over the Internet. We like the added

protection of the GCR420. What are the Keyboard Vendors that this reader supports and computers as well? I'm ready to order this for this pilot. What can I do?

Regards,

Todd Lewis
Information Dynamics
tlewis@idinc.com
phone: (202) 863-5201 Ext 106
Pager: 888-929-7937

INFORMATION AUTOMATIC VIRUS CHECK (GEMPLUS) No virus
known.

4.7 Status of Support for Adobe Acrobat Exchange 4.0 in HAHTsite

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

From: Michael Kelley [<mailto:michaelk@haht.com>]
Sent: Friday, April 23, 1999 11:15 AM
To: TLewis@idinc.com
Subject: RE: FW: Support needed for EPA Pilot (Incident #37410)

Todd,

We will be testing the HAHTsite Adobe ESM with Exchange 4.0 within the next 2-3 weeks. For a variety of reasons, we're just not going to be able to get to it any sooner than that.

We would expect, however, that the existing Adobe ESM will work with Exchange 4.0 and Acrobat Reader 4.0. Are you able to at least give it a try and see if any problems occur? At the moment, the existing ESM is what has the best chance of working, since we have not yet done testing with the 4.0 versions.

We're also not aware of a solution to your problem when using the Acrobat/Exchange 3.0 components.

I apologize for not being able to offer any better help here. You're just a little ahead of us in needing to run with the 4.0 components because of the problems with the 3.0 components.

Michael Kelley
Vice President of Software Development
HAHT Software

From: Lewis, Todd
Email: TLewis@idinc.com
To: SMTP:daveh@haht.com
Cc:SMTP:WLiu@idinc.com;SMTP:AYang@idinc.com;SMTP:JeannetteD@haht.com;
SMTP:support@haht.com;SMTP:idi-epa@elock.com
Date: Thursday, April 22, 1999, 5:54PM
Subject: RE: FW: Support needed for EPA Pilot

Dave, no, I do mean Adobe Acrobat Exchange forms. Only the Adobe Acrobat Exchange forms allow the types of third-party plug-ins which can be used to digitally sign the contents of the Adobe PDF form as it exists in the memory of the computer at the time the signer is viewing the form. We are using Adobe Acrobat Exchange plug-ins from E-Lock Technologies, Inc., (for cryptographic digital signatures) and PenOp (for biometric handwritten signature dynamics). The issue for Haht Software is that Haht Software's technical support has stated that HAHTsite has not been tested for compatibility with Adobe Acrobat Exchange forms 4.0. [We are currently using Adobe Acrobat Exchange forms 3.01.] We need to have a development beta (or whatever is available) of the Haht Software Adobe-related components for HAHTsite which has the best chance of working with the Adobe Acrobat Exchange 4.0 product (or alternatively, a method of successfully working with Adobe Acrobat Exchange forms Version 3.01 and Internet Explorer 4.0 in the HAHTsite environment).

Thank you,

Todd
TLewis@idinc.com

4.8 *Multiple Adobe Form Windows in Internet Explorer and Duplicate Record Insertion when Storing Form Data using HAHTsite Programming*

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

From: Lewis, Todd
Sent: Thursday, April 22, 1999 3:44 PM
To: 'Dave Hock'
Cc: Liu, WeiShing; Yang, AnPing; 'Jeannette Durrett'; 'Haht Software

Support'; 'IDI-EPA Distribution'

Subject: RE: FW: Support needed for EPA Pilot

Dave, we are nearing production installation of a highly visible pilot project sponsored by the U.S. Environmental Protection Agency in the State of New York for the Internet submission of environmental compliance data using an Adobe Exchange PDF form within a browser environment. The success or failure of this pilot may have a great deal to say in how the EPA and the rest of the federal government implement their electronic reporting standards and requirements. We are using the HAHTsite application server at the receiving Web site. We have been working with Haht Software technical support, but I am hoping that you may be able to provide additional help in resolving a major unsolved issue:

When an Adobe Exchange PDF form template (Version 3.01) is prepared using the Haht IDE environment and then downloaded to the client within Microsoft Internet Explorer 4.0, then it opens in a new Internet Explorer Window and the Adobe Exchange form application (Version 3.01) is launched as a helper application to view the PDF form. So far--so good--but if this process is repeated, then another instance of the Adobe Exchange form application is launched (because the previous instance of the Adobe Exchange form is not closed). At some point (usually the second time) in the process of opening new IE windows and launching new instances of the Adobe Exchange form application, the Adobe Exchange form fails to load or display the PDF form.

A manual experiment has confirmed that if the previous instance of the Adobe Exchange form application is manually closed by the user, then the process of opening new PDF forms can proceed indefinitely (although accumulating multiple unclosed IE windows). We need a more elegant solution than to tell all Internet Explorer users in the New York pilot to constantly close previous instances of Adobe Exchange as they prepare and submit environmental compliance forms. At least one newsgroup discussion identifies this problem and claims that Adobe Exchange Version 4.0 solves this problem. I understand that Haht technical support says they are working on testing Adobe Exchange 4.0 with HAHTsite, but don't have a definitive result.

Given the imminent production deadline and visibility of this project, would there be anyway that we could have some advance notice on preliminary results of your tests or a

beta version of the HAHTsite components which could work with Adobe Exchange 4.0? Alternatively, is there a way to force Adobe Exchange form Version 3.01 to exit after the FDF data stream has been sent to the HAHTsite server?

Thank you in advance for your attention to this matter,

Todd
Dr. J. Todd Lewis
Program Manager
Information Dynamics, Inc.
400 Virginia Ave., Suite 110
Washington, DC 20024-2730
(202)-863-5201 Ext. 106
(202)-863-5210 (fax)
1-(888)-929-7937 (pager)
TLewis@idinc.com

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

From: Dave Hock [<mailto:daveh@haht.com>]
Sent: Monday, January 25, 1999 3:17 PM
To: Lewis, Todd
Cc: 'Dov Cohn'; 'Jeannette Durrett'
Subject: Re: FW: Support needed, demo web page on 1/28/99.

Hi Todd.

The best thing to do is call our support line or send a note to support@haht.com.

Also note that Dov is no longer with the company. You can contact me for Adobe related issues.

Dave Hock

Lewis, Todd wrote:

Dov, what is the best mechanism to obtain technical support related to the Environmental Protection Agency's electronic reporting pilot? We have purchased the HAHTsite IDE and application server licenses with software maintenance.

Thank you,

Todd
TLewis@idinc.com

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

From: Weisheng Liu [mailto:wliu@discovery.idinc.com]
Sent: Monday, January 25, 1999 9:11 AM
To: brants@haht.com; dovcc@haht.com
Cc: TLewis@idinc.com
Subject: Support needed, demo web page on 1/28/99.

Hi,

I Need Help.

The following code always inserts a duplicate record, one after another - If I insert one record only, a duplicate set of records is created after another set.

Why?

```
For loopCount = 1 To xNumOfSample
  tmpStr = "(" & trim$(Str$(loopCount)) & ")"
  commons.AddNew
  commons("pkFacility") = keyFacility
  commons("NPID") = keyNPID
  commons("PLDS") = keyPLDS
  commons("PLRD") = keyPLRD
  commons("MSDT") = keyMSDT
  commons("MVDT") = keyMVDT
  commons("PRAM") = WebApp.URLField$("txtPRAM" & tmpStr)
  commons("MLOC") = WebApp.URLField$("txtMLOC" & tmpStr)
  commons("SEAN") = WebApp.URLField$("txtSEAN" & tmpStr)
  commons("MODN") = WebApp.URLField$("txtMODN" & tmpStr)
  commons("MQAV") = WebApp.URLField$("txtMQAV" & tmpStr)
  commons("MQMX") = WebApp.URLField$("txtMQMX" & tmpStr)
  commons("MCMN") = WebApp.URLField$("txtMCMN" & tmpStr)
  commons("MCAV") = WebApp.URLField$("txtMCAV" & tmpStr)
  commons("MCMX") = WebApp.URLField$("txtMCMX" & tmpStr)
  commons("REXC") = WebApp.URLField$("txtREXC" & tmpStr)
  commons("RFRQ") = WebApp.URLField$("txtRFRQ" & tmpStr)
  commons("RSAM") = WebApp.URLField$("txtRSAM" & tmpStr)
  commons("Version") = keyVersion
  commons.Update
  Next loopCount
```

- combine 11 field as primary key. keyNPID, key... and
WebApp.URLField\$("txtPRAM" & tmpStr),
WebApp.URLField\$("txtMLOC" & tmpStr),
WebApp.URLField\$("txtSEAN" & tmpStr),
WebApp.URLField\$("txtMODN" & tmpStr) for single record.

- keyFacility, keyNPID, keyPLDS, keyPLRD, ketMSDT, keyMVDT

is single record which displays on multiple PDF pages. For Database Query Page; Number of Repeating Fields; What's the number I should put in there? 0 or Number of pages displaying such fields? I have tried all the combinations: 0, 1 and number of page(s). Duplicate record insertion happened in each case.

- AddNew and Update. Is there any trick between them?

Thank you for your assistance.

Weishing Liu.

Deliverables 4.1 & 4.2, Information Dynamics, Inc.

¹ 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.

² Submission of Environmental Data Under the Taiwan-USEPA Technical Cooperation Agreement