

B8595HC
2. C56
Copy 1

**Project: Corresponding with Customers Via Electronic Mail
For Business Personal Property PT-100 Return Data
South Carolina Department of Revenue**

**Pamela Steele
South Carolina Department of Revenue
January 28, 2005**

S. C. STATE LIBRARY

AUG 22 2005

STATE DOCUMENTS

Executive Summary

In the Fall of 2004, an assignment was made by the director of the Information Resource Management (IRM) division to determine if corresponding with taxpayers via email was a feasible secure communication method. After this assignment was made monthly Business Personal Property PT100 return data process was thought to be a good candidate for the new process. Currently, DOR sends monthly Business Personal Property PT100 return data created on a diskette to taxpayers depending on their accounting period via U.S. Mail. The tax preparer completes the return information on the diskette and then mails the diskette back to DOR. The diskette is delivered to the mail room and then sent to the Electronic Services section. A pre-edit is performed on the data and if no errors are detected on the file, a run sheet is completed and delivered to the computer room. The file is then uploaded to the mainframe and processed. The update process is then complete for that taxpayer until the next year. If there is a problem in either the pre-edit or update process, the data must be corrected. Sometimes this requires the diskette to be sent back to the taxpayer via U. S. Mail and the process will start over.

The result of this project will be to instruct Business Personal Property PT-100 return preparers how to receive and reply to encrypted emails sent from and to DOR that contains confidential taxpayer information. This process will eliminate the need to mail the return data to and from the tax preparer. Instructions will explain the steps involved in transmitting the PT-100 data utilizing the TESS email encryption software. This option will provide another customer friendly option to communicate with stakeholders.

TABLE OF CONTENTS

- I. Executive Summary**
- II. Introduction**
- III. Purpose of Project**
- IV. Information Sources and Methodology**
- V. Results**
- VI. Summary and Conclusion**
- VII. References**
- VIII. Attachments**
 - 1. Attachment 1 - Current Process**
 - 2. Attachment 2 – Proposed Process**
 - 3. Attachment 3 – Proposed One Time Process**

**Project: Corresponding with Customers Via Electronic Mail
For Business Personal Property PT-100 Return Data
South Carolina Department of Revenue**

Introduction

Many public and private businesses use electronically transmitted information as a fast, efficient and documented way of communication. The South Carolina Department of Revenue (DOR) relies on electronic mail (e-mail) for communicating with taxpayers when responses to inquiries are sent in via the web site. E-mail can be defined as the transmission of messages over communication networks.¹ Electronically transmitted information travels through many networks and many different computer connections. During the transmission of data from the sender to the recipient the message could be intercepted by a third party. Unless encrypted this information is not secure. Encryption is defined as the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.² The process of encrypting data simply means to make it unreadable to anybody except the intended recipient. DOR handles confidential taxpayer information such as social security numbers, federal identification numbers, and tax due or paid amounts. DOR has to be

¹ Webopedia.com (Online dictionary)

² Webopedia.com (Online dictionary)

accountable to customers and be responsible for all actions in handling sensitive taxpayer data.³

Purpose of Project

In the Fall of 2004, an assignment was made by the director of the Information Resource Management (IRM) division to determine if corresponding with taxpayers via email was a feasible secure communication method. The method should consider getting and keeping current email addresses, legal issues, and taxpayer privacy. The following key results of DOR'S Strategic Plan cover actions needed in this project.⁴

1. Maximized Compliance - Provide quality customer service.
2. Strong Stakeholder Relationships - Provide a variety of customer-friendly options to communicate effectively with stakeholders.
3. Effective and Efficient Agency and Enterprise Services - Continuously evaluate and implement innovative technology to improve the quality and speed of service delivery while minimizing cost.

Currently, DOR sends monthly Business Personal Property PT100 return data created on a diskette to taxpayers depending on their accounting period via U.S. Mail. The taxpayer or tax preparer completes the return information on the diskette and then mails the diskette back to DOR. The diskette is delivered to the mail room at DOR and then sent to the Electronic Services section. A pre-edit is performed on the data and if no errors are detected on the file, a run sheet is completed and delivered to the computer

³ South Carolina Code of Laws – Title 12 - Taxation Chapter 54 – Section 12-54-240(A)

⁴ South Carolina Department of Revenue Strategic Plan

room. The file is then uploaded to the mainframe and processed. The update process is then complete for that taxpayer until the next year. If there is a problem in either the pre-edit or update process, the data must be corrected. Sometimes this requires the diskette to be sent back to the taxpayer via U. S. Mail and the process will start over.

In December of 2004, Tovariss TESS SecureMail Gateway (TESS) email encryption software was purchased by DOR. TESS is an email encryption solution that works with DOR's existing network and application infrastructure. With TESS, sensitive information in email messages can be sent securely to any recipient anywhere in the world at anytime. TESS is a computer that sits between DOR's email server and the Internet. Normally when a regular email is received, it is sent from the sender's computer to a server computer in the sender's organization, which sends the email to the Internet. With TESS, when DOR sends a secure email across the Internet, the message will go to the TESS server where it will be encrypted.

The purpose of this project is to instruct Business Personal Property PT-100 return preparers how to receive and reply to encrypted emails sent from and to DOR that contains confidential taxpayer information. The instructions will explain the steps involved in transmitting the PT-100 data utilizing the TESS email encryption software. The instructions will be divided into four steps: an overview, sending encrypted emails, verifying that received emails have been encrypted and review. The first step, the overview, will introduce the content of each chapter and the reason why encrypted email is needed. The next chapter will explain the method to send an encrypted email message. The third chapter will discuss how to tell if a received email message has been encrypted. The last chapter will be a review of the email concepts and procedures.

Information Sources and Methodology

To gather information on what other states were doing with secured email, an inquiry was sent to the Federation of Tax Administrators (FTA) in Washington DC. The FTA serves as a source of information and expertise for state administrators and others on the workings of state tax agencies and systems as well as issues generally affecting tax policy and administration. FTA staff regularly monitors the activities of state tax agencies and the federal government in order to serve as a clearinghouse on topics important to administrators. FTA also conducts research projects in such area as state tax policy and structures, compliance and enforcement programs, and federal and state court decisions. In addition significant effort is devoted to inquiries from tax administrator on special problems and issues.⁵

The following questions were sent to FTA for comments from others states:

1. What are you sending via email?
2. How are you handling security for confidential information?
3. How are you gathering email addresses? Are they accurate?
4. Overall, how is the use of email working for your agency?

Eleven states responded to the request for information. Out of the eleven responses, eight states were doing less with secure email than DOR. The other three states responded with useful information. The Colorado Department of Revenue (CDOR) collects email addresses from tax class attendees and tax professionals when they attend a class. Also, the CDOR website offers taxpayers a subscription to receive emails on promotional information. Then an email address is received, the CDOR adds the email address to

⁵ Federation of Tax Administrators website: Research and Information Exchange
<http://www.taxadmin.org/fta/ftafact1.html>

their database. The taxpayer has the option to opt out of the email service at anytime. CDOR stated that for the most part they have accurate email addresses. There will always be an effort to keep the email addresses correct. CDOR feels that it is worth the effort to get and keep current email addresses. Very few taxpayers want to discontinue receiving emailed information. Tax professionals have commented in meetings that they very much appreciate the information CDOR sends via email.⁶

Michigan Department of Revenue (MDOR) is also using secure email to correspond with taxpayers. MDOR accepts emails from taxpayers who have first inquired through the self-service web connection. When the taxpayer requests information via email, a unique identifier is assigned by the secured email software. Before any secured information is given a second step is taken to identify the taxpayer. The taxpayer is asked questions that only the taxpayers should know. For example, what is your adjusted gross income from last tax year? MDOR collects email addresses on their business registration application, call center and through the web self-service system. MDOR has been corresponding with taxpayers via secured email for less than a year and the business community has received it well.⁷

Virginia Department of Revenue (VDOR) has used a custom application called Secure Messaging to correspond with taxpayers via email since January 2002. The Secure Message Center is a secure communication channel that provides taxpayers the ability to request and receive confidential information via email. The messages to and from the taxpayers are encrypted. The taxpayer must first answer questions that only they should know. After the taxpayer has been authenticated, they can compose and

⁶ R. Giardini , Colorado Department of Revenue (personal communication, August 24, 2004)

⁷ Liz Chaney, Michigan Department of Revenue (personal communication, September 9, 2004)

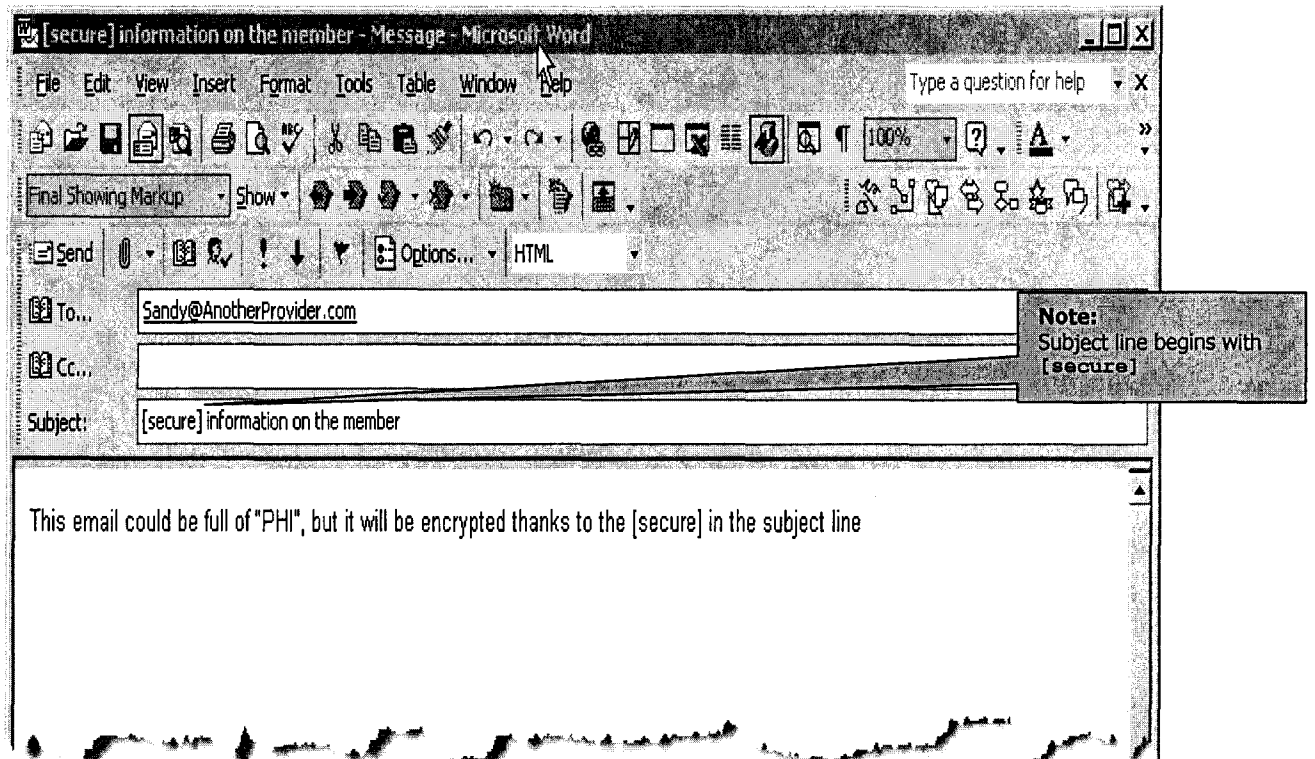
transmit secure messages to VDOR. Then VDOR can compose and transmit secure replies back to the taxpayer. An email alert through traditional email notifies the taxpayer when he has an update on his Secure Message Center. VDOR has received over 10,000 secure email messages from taxpayers from January 2004 to July 2004.⁸

Results

After reviewing the current process of sending the PT-100 return data on diskettes to taxpayers via U. S. Mail, it is suggested that the data be sent via secured email. It is also suggested to start with a small group of taxpayers so the process can be monitored until the process is familiar to all users. The taxpayer will need to be contacted by telephone or letter to see who is interested in the new secured email process. After an interest is indicated, the taxpayer will need to provide his email address to DOR. This process can be done by letting the taxpayer send an email to the Electronic Services area of DOR. This process will reduce the possibility of keying the wrong email address. Once the email is received it can be stored in a designated email address folder for later use. Then DOR will give the taxpayer a password or pass phrase to be used to open the secured email. The taxpayer will also need instructions on how to receive and respond to secure emails from DOR. A taxpayer knows he has received a secure email when the word secure is in square brackets in the subject line. See example below:

⁸ F. Beaton, Virginia Department of Revenue (personal communication, August 24, 2004)

Example 1: Example email message with [secure] in subject line



Next, information needs to be gathered by the sender that will create a key which will be used by the recipient to decrypt the message. This information that has been completed by the sender requires information known only to the recipient that will serve as the key to decrypt the email. See the following example of the questions to be used as the key:

Example 2: Example of key questions.

Welcome to SecureMessenger™!

You have elected to send the following e-mail message securely:
Subject: information on the member
To: Sandy@AnotherProvider.com

Please provide the following additional information:

1. Enter a clue that will enable the recipient to determine the password or passphrase that you will enter in step 2.
Required:
2. Enter the secret password or passphrase that will allow your recipient to unlock your message.
Required:
3. Your message will be available to the recipient for a limited time. Please choose how long you want the message to be accessible.
Required:
4. You may request that a notification message be sent to you when the recipient unlocks and views your message for the first time.
Optional: Send me a read receipt.
5. You may specify that these same values (password or passphrase, clue, and message lifetime) be used every time you send a secure message to this recipient.
 You may also invite the recipient to set up their own clue and passphrase.
 - Only use these values this time.
 - Use these values whenever I send secure mail to Sandy@AnotherProvider.com.
 - Use these values whenever anyone in my organization sends secure mail to Sandy@AnotherProvider.com.
 - Use these values and invite the recipient to set up their own values for future secure email.

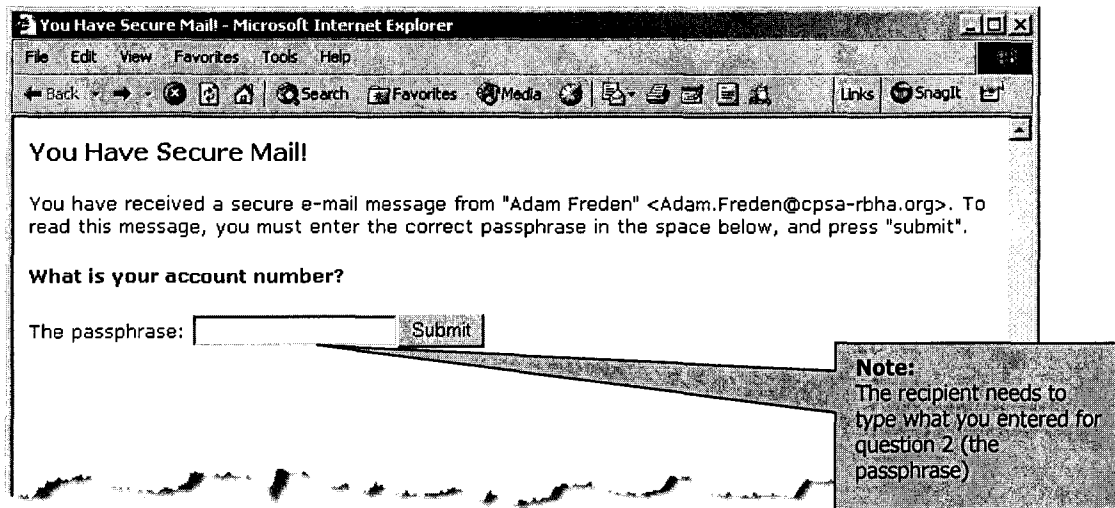
The first two questions will create the information for the key:

- The answer to question one will be obvious for the recipient, but nobody else.
- The answer to question two is the actual key.
- Question three tells the recipient how long the email can be accessed. (Recipient has the option of saving the message to their computer).
- Question four informs the sender when the encrypted email has been accessed by the recipient.
- Question five asks if the values above should be used automatically whenever secured emails are sent to the recipient.

After the sender answers the questions and sends the email, another email message will appear from TESS. This second email will inform the recipient that an encrypted email is waiting for them, and that they now need to access an encrypted web page. The recipient will then be asked to enter their password or pass phrase one more time. This is the same

as question 2 in Example 2. The following is an example of the screen that will be displayed to enter the password or pass phrase.

Example 3: Web page showing need to enter password or pass phrase.



After the password or pass phrase is entered and submit button is depressed, the web page with the PT-100 data will be displayed. The recipient will be able to now access it.

The recipient can now take the PT-100 data and update it. Then the updated data is ready to be sent back to DOR, the recipient can attach a file of the updated data to the encrypted email and send it back to the sender. The Electronic Section of DOR will receive the email with the PT-100 data attached. The file is then processed in its normal way.

Summary and Conclusion

The new process seems like a lot of steps to through to get a file, but it will save both the taxpayer and DOR valuable time. Receiving and sending an email and answering a few questions should take very little time. No time will be wasted sending

and waiting on diskettes to be mailed. The steps to receive and send encrypted emails maybe done without leaving the office and within a few minutes. There will be no worry that the diskette gets lost in the mail. The taxpayer and DOR will be assured the data was been received by the other party since an email is sent verifying the delivery of the data.

One recommendation is to add a screen to DOR's website for taxpayers and tax preparers to request information via email and register their email addresses. Also make a better effort to collect email addresses during classes and seminars. Additional information on educating the taxpayer in how email can be used in correspondence could be added to DOR's website. Through an effort to obtain and maintain email addresses DOR could provide another customer friendly option to communicate with stakeholders.

References:

Webopedia.com (Online dictionary)

South Carolina Department of Revenue Strategic Plan

R. Giardini, Colorado Department of Revenue (personal communication, August 24, 2004)

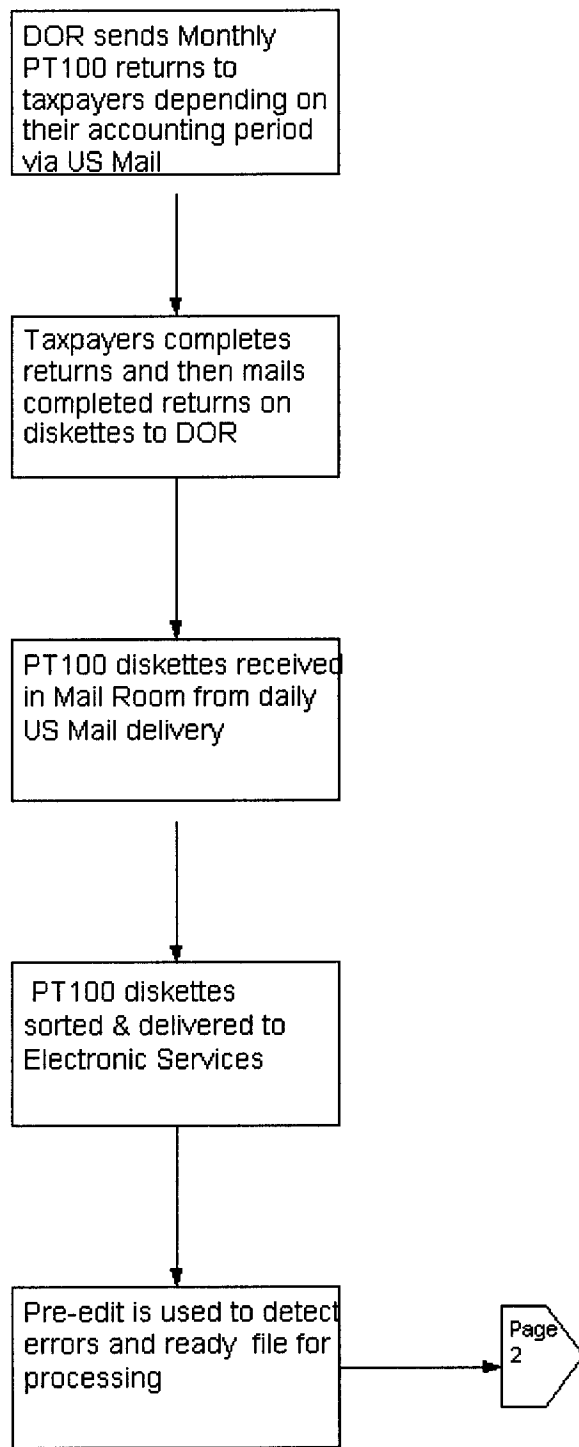
Liz Chaney, Michigan Department of Revenue (personal communication, September 9, 2004)

F. Beaton, Virginia Department of Revenue (personal communication, August 24, 2004)

ATTACHMENT 1

Current process using US Mail delivery
Business Personal Property - PT100 Diskette Filing

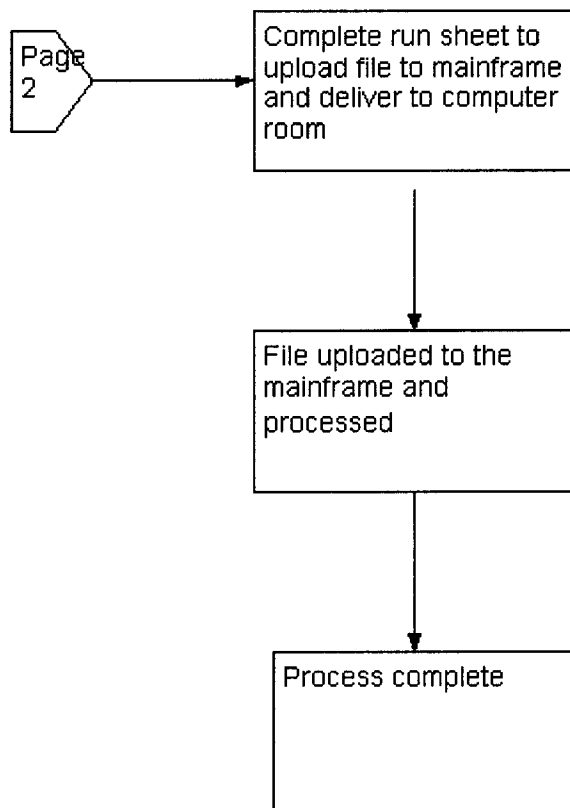
Page 1 of 2



ATTACHMENT 1

Current process using US Mail delivery
Business Personal Property - PT100 Diskette Filing

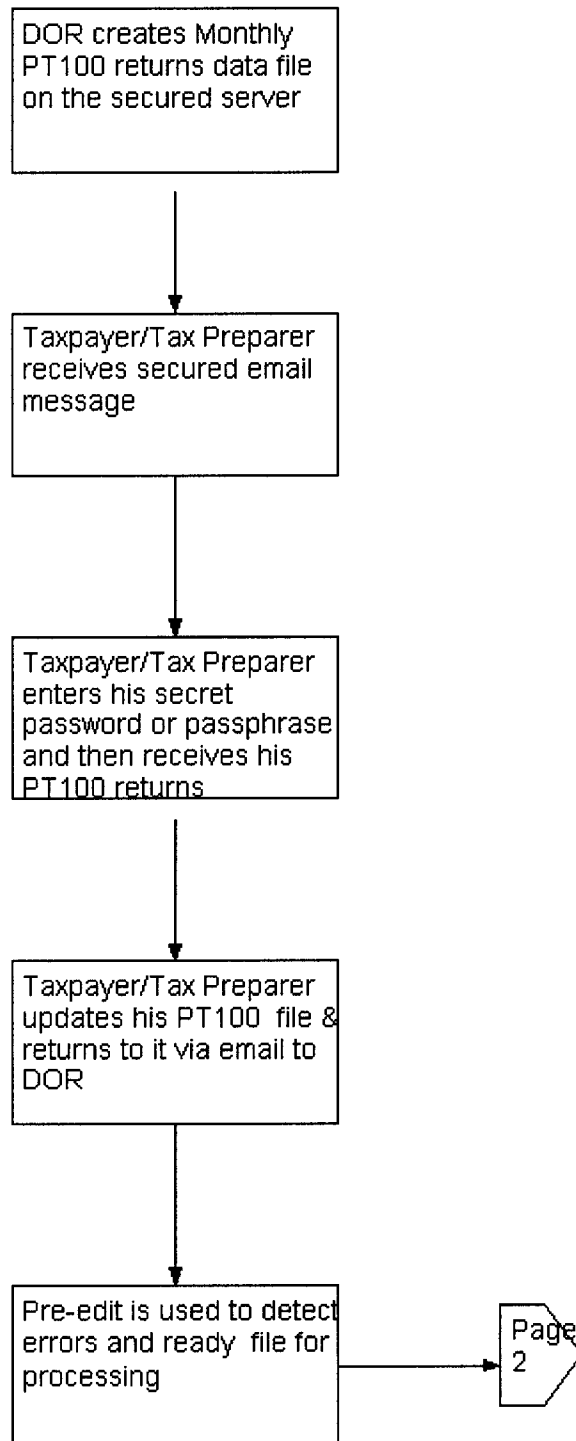
Page 2 of 2



ATTACHMENT 2

Proposed process using Secured Email
Business Personal Property - PT100 Filing

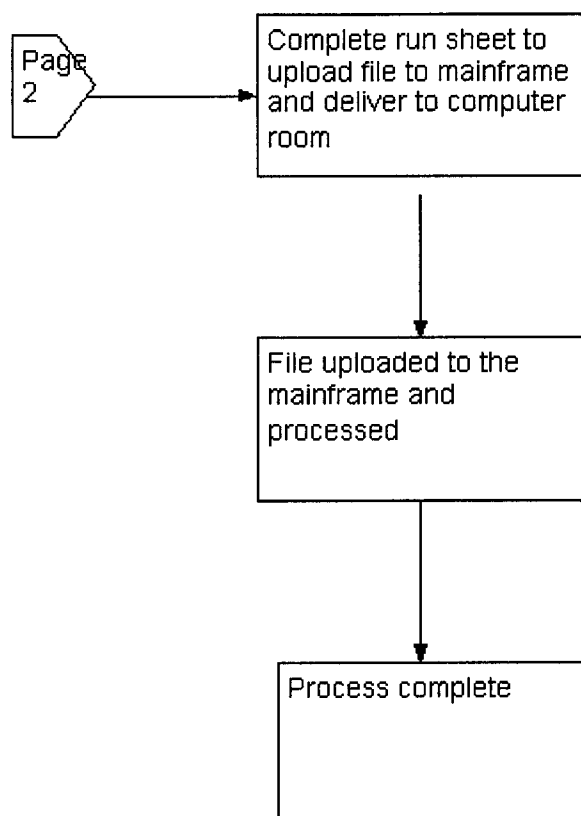
Page 1 of 2



ATTACHMENT 2

Proposed process using Secured Email
Business Personal Property - PT100 Filing

Page 2 of 2



ATTACHMENT 3

Proposed Process to Set-up Taxpayer's User-id and Password
(One-Time Process)

Page 1 of 1

