

***Encryption Implementation
at the
Tennessee Department of Revenue***

**Federation of
Tax Administrators
August 2007**

Contact Info

Gordon Smead

Gordon.Smead@state.tn.us




(615) 741-8355

Bart Wallace

Bart.Wallace@state.tn.us

(615) 741-9084

A quick look at:

-  The Tennessee Department of Revenue's Need for Encryption.
-  How We Went about Procuring an Encryption Solution.
-  How Our Implementation Has Gone So Far.

The Tennessee Department of Revenue's Need for Encryption

**Tennessee does not
want to be on television
broadcasts about
compromised
taxpayer data:**

• **Veterans' data stolen**



**Bob Sullivan explains
how information was
put at risk.**

According to Robert McFarland, VA assistant secretary for information and technology:

- **“Data removed from computer systems onto devices such as laptops should be encrypted.”**
- **“If it was encrypted, then it's going to be useless to anybody, but [the VA cannot say that] it was encrypted.”**

Tennessee does not want to be in newspaper articles about compromised taxpayer data:

State X: **Taxpayer Data Missing**

Jun 28, 2006 3:38 pm US/Central

(AP) ... [State X] tax officials disclosed Wednesday that private information on 50,000 taxpayers -- mostly businesses being audited for back taxes -- has been missing for more than a month.

Social Security numbers and other information for 2,400 individual taxpayers and identifying information on 48,000 businesses were lost.



**The Tennessee
Department of Revenue
doesn't want to be in
blogs about
compromised
taxpayer data:**

State Y: Taxpayer Data Lost!

DATA LOST

Laptop theft puts residents at risk
Computer had files on 30,000 ...
taxpayers

... A laptop computer containing files on 30,000 taxpayers was stolen from the car of a ... **[State Y]** Department of Revenue employee last month, and state officials are cautioning everyone on the list to keep an eye on their finances for potential fraud.



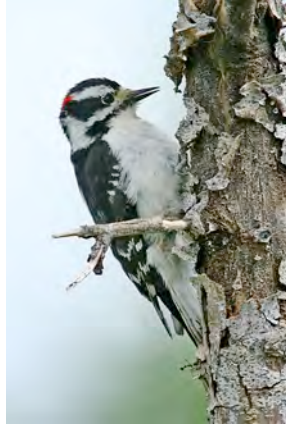
Tennessee does not want
to be involved in lawsuits
about compromised
data:



Bottom Line:

Tennessee does not want to compromise data!

[Knock on Wood]



We must secure data on the

- laptops [550 assigned now, 450 with wireless cards]
- flash drives
- and other portable media

used by Revenue employees throughout the state and across the nation.

We Have Department of Revenue Offices throughout Tennessee ...



- Chattanooga
- Columbia
- Cookeville
- Humboldt
- Jackson
- Johnson City
- Knoxville
- Nashville
- Memphis
- Shelbyville

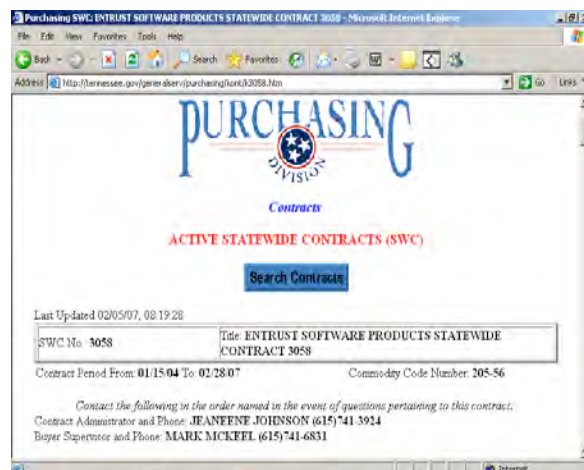
... and across the Country, Including:

- Atlanta
- Boston
- Chicago
- Cincinnati
- Cleveland
- Houston
- Newport Beach
- NYC
- Philadelphia



2. How We Went about Procuring an Encryption Solution

First we looked up what was on State contract ...



... including software costs ...

Contract Items and Services for SWC #3058

Unless specified elsewhere, ship to: Statewide
Commodity Codes in hypertext links below, if clicked, will lead to a picture of the product!

| SWC No. | Contract No. | Line No. | Commodity Code | Unit | Unit Price | Discount Off Catalog Price |
|-----------------|--------------|----------|--|-------|------------|----------------------------|
| 3058 2050351 | 4031011 | 00001 | 205-56-045196 Software - Entrust Technologies (percent Mark Up Or Discount From Catalog Price) Catalog Entrust Technologies Product (Offerings Dated October 29 2003 Catalog May Be Obtained From Laurie Gowling 613-270- 3453 | APCAT | \$0.00000 | N/A |

Vendor: **Entrust** Recycle Content: N/A
 Contract extended to Local Governments & State Agencies

... and maintenance support.

| | | | | | | |
|-----------------|---------|-------|---|-------|-----------|-----|
| 3058 2050351 | 4031011 | 00003 | 948-07-045205 Software Maintenance And Support (to Include But Not Limited To Telephone Support Levels Technical, Basic, And Emergency Support) Entrust Technologies (percent Mark Up Or Discount From Catalog Price) Unit Apcat = As Per Catalog | APCAT | \$0.00000 | N/A |
|-----------------|---------|-------|---|-------|-----------|-----|

Vendor: **Entrust** Recycle Content: N/A
 Contract extended to Local Governments & State Agencies

Then Revenue staff, along with State of Tennessee security administrators, met with Entrust personnel.

We had a detailed discussion about how Entrust's solution works.

With our State security director satisfied with the product, we moved ahead on the project.

We finalized our project plan ...

SMALL PROJECT

| | |
|--|--|
| Project Name: Software Encryption Sponsor/Contact: Sam Chessor/Gordon Smead Agency/Division: Revenue/Administration | Project Number: DG283 Project Fiscal Year: 2006/2007 Priority: 36 Funding Source Initial Costs: SC Funding Source Operational Costs: SC |
| Business Goal or Objective: Objective 2.1: Establish and communicate smart tax policy so people understand the department's position. Strategy 2.1.4 of this objective calls for us to utilize technology to communicate our message. In our use of technology, we need to protect our data. The intent of this project is to ensure that all confidential State information on portable media and computers is encrypted to prevent security breaches in the event they are lost or stolen. | |
| Functional & Technical Description: Revenue needs to encrypt information on portable media and computers to comply with enterprise information security policy and to safeguard confidential information. Entrust is the sole provider of such software on State contract. | |

| Initial Costs | | | |
|---|--|----------------|-----------|
| Cost Category * | Description | Existing Costs | New Costs |
| Personnel | Departmental IS staff time for analysis, design, programming, testing, training, and implementation. Estimated at 50 hours (\$36/hour) | | \$1,800 |
| Software | Entrust Intelligence Disk and Media Security (550 licenses) | | \$81,950 |
| Hardware | | | |
| Security | | | |
| Communications | | | |
| Training | | | |
| | Totals: | | \$83,750 |
| Operational Costs | | | |
| Cost Category * | Description | Existing Costs | New Costs |
| Personnel | | | |
| Software | Third Party Pointsec Support Silver support calculated at 18% for 1 year | | \$14,751 |
| Hardware Replacement | | | |
| Security | | | |
| Communications | | | |
| Hosting Services | | | |
| | Totals: | | \$14,751 |
| Total Initial (New + Existing) | | | \$83,750 |
| Total Operational (New + Existing) | | | \$14,751 |

... and costs.

After receiving final Management Advisory Committee approval for 550 licenses, we placed our order with Entrust.

We ordered 550 licenses for Entrust Entelligence Disk and Media Security for \$81,950.

We purchased Third Party Pointsec Silver Support, calculated at 18% for 1 year, for \$14,751.

Entrust Contacts

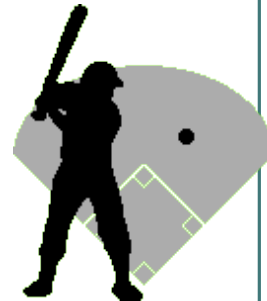
John Lister, 404-372-0266, is Entrust's sales manager for Tennessee.

Ernie Tarbox, 704-548-1080, is Entrust's systems engineer. Ernie proved to be a great help in showing us how to implement Entrust's encryption package.

3. How Our Implementation Has Gone So Far

First of all, Bart Wallace, one of our outstanding information resources support specialists, was made project lead of this implementation.

Bart has been
“knocking ‘em out of the
park”
on this project.



We've been given unique IDs by Entrust to download administrative manuals and customer support materials.

We've assigned 6 contacts to provide technical support for encryption.

To assist in resuming staff with encrypted equipment who get 'locked out', we set up a challenge database asking questions such as:

**What city were you born in?
What is your mother's maiden name?
What is your favorite color?
What was your first pet's name?
Where did you attend high school?**

We've established a process that our Integrated Help Desk staff may follow to help make such resumptions.

We have a policy on personal storage drives and a form that Revenue Staff must complete prior to being authorized to use flash drives:

Flash Drive Form

To protect the confidentiality of State of Tennessee taxpayer information, the Department of Revenue will encrypt the hard drive in all portable computers as well as any desktop computers which will be sharing confidential information. Software also will be installed to facilitate encryption on all portable storage devices.

If taxpayer information is saved to this flash drive it will be encrypted using the State Standard Software of media encryption called Entrust. This encryption software will prevent unauthorized access to confidential information stored within the system.

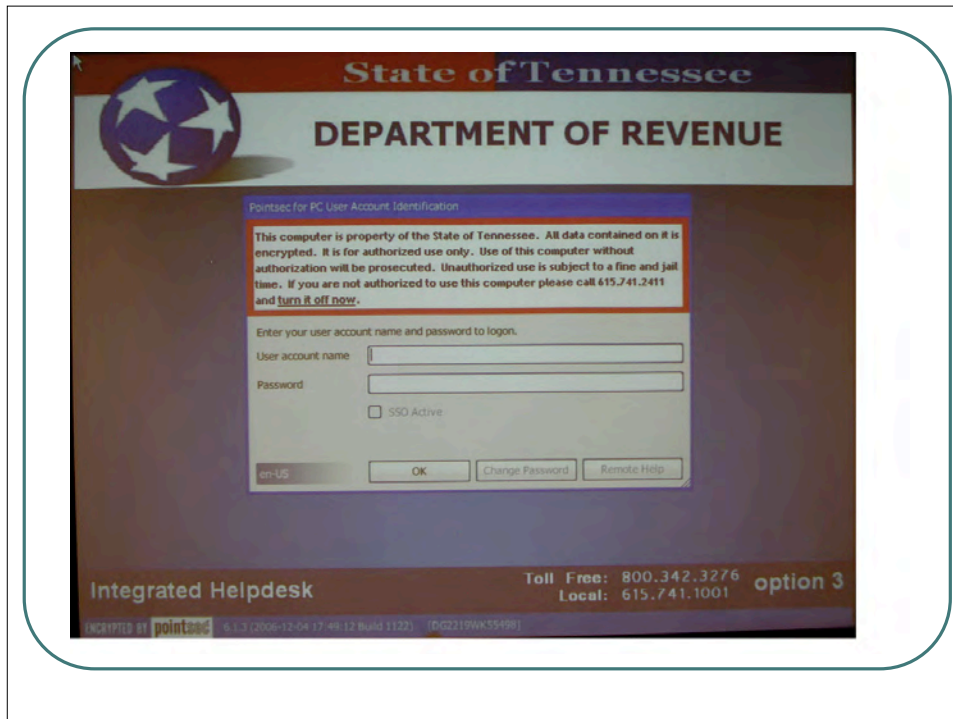
In the instance of a taxpayer being given their confidential information via other external media, the data will be encrypted and password protected using Pointsec encryption packages. In these instances, the password will be given to the taxpayer in order for them to view the data since they do not have our encryption software.

It is against Departmental Policy to use personal storage drives [or to use departmental drives for personal information storage](#). More information on the [use and restrictions on use of portable storage devices](#) can be found in the Computer Guidelines on [page 11](#), under the section titled Mobile Device Encryption.

Our Mantra

**“Cyber Security is
Everyone’s
Responsibility!”**

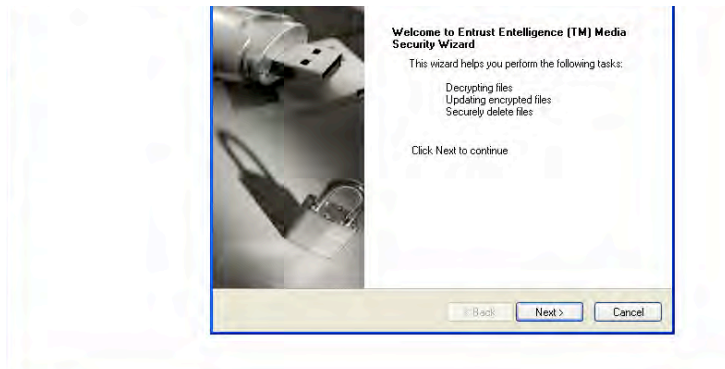
**Here’s what our pre-boot
sign-on screen for
encrypted equipment
looks like:**



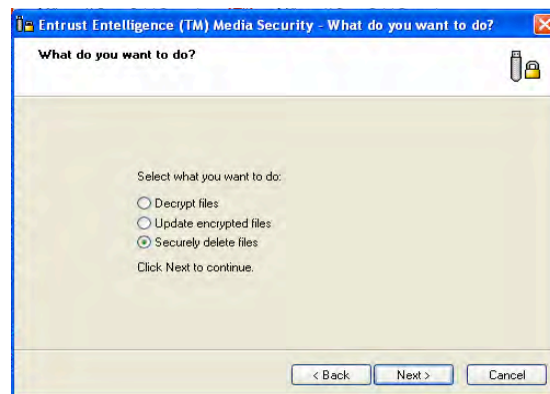
Here's What the Media Security Password Screen Looks Like:



Here's How the Media Security Wizard Works:



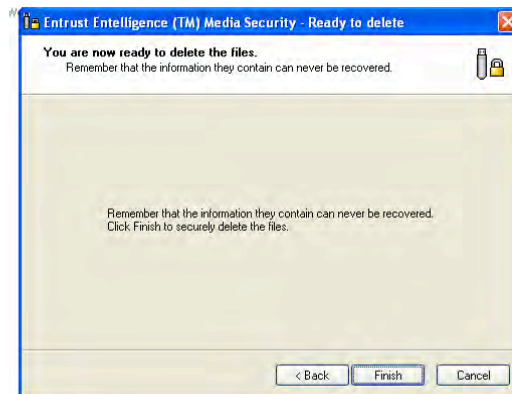
Here We Choose to Securely Delete Files:



Here We Specify the File to Delete:



Warning Prior to Deletion:



Completed



Bart Wallace

There was much detailed work involved in this project.

Bart will cover some of the hurdles we had to jump in getting everything running and then we'll close with a question and answer session.

Testing and Implementation



During testing we found no software compatibility issues with Disk Security or Media Security and no hardware devices were adversely affected.

Testing and Implementation (Continued)

All software has remained fully functional and there has been no interference with critical updates or Symantec Antivirus functionality.

Testing and Implementation (Continued)

All communications via e-mail and between the encrypted computers and various servers remains unaffected. Also, the encryption software does not noticeably slow the computer's operation.



Testing and Implementation (Continued)

We now have about 550 mobile computers in use with Disk Security and Media Security installed. We started placing it in production in November 2006.

Testing and Implementation (End of this Section)

We install from a Novell file server, mainly so that changes can be made from a central location that all of our users have access to.

The recovery files are copied back to the server during the installation process. Profile updates, when necessary, can be made available from the same location.

Support issues

There have been relatively few support issues. The Entrust web site has some good support information available on it. Service requests that have been submitted to Entrust have been resolved promptly with good results.

Support issues (Continued)

The Remote Help procedure functions well when people call for help with a locked account. Access to the network is unnecessary in order for users to receive Remote Help for Disk Security at pre-boot, because it is a challenge/response process.

Support issues (Continued)

The same goes for password help with Media Security protected data, except techs providing assistance are required to access the stored recovery file for each computer.

This is why it is important for Media Security recovery files to be stored successfully in a safe location.

Support issues (Continued)

Disk Security recovery files mainly are used to remove encryption when a problem prevents software from performing that function and data must be recovered.

Support issues (Continued)

**In testing, this worked well.
We were able to decrypt and recover data using a recovery disk created from the recovery file.**

Support issues (Continued)

In production, however, this has failed on occasion when a hard drive has bad sectors on it. This is not due to a failure of the encryption process, however, because the problem that made decryption necessary was caused by the failed hard drive.

Support issues (Continued)

This brings up another point. Hard drives that are being encrypted need to be healthy. It is time-consuming to defrag and disk-check every computer that you plan to encrypt, but it may be worthwhile.



Support issues (Continued)

It is also advisable, at a minimum, to back up all important data to a safe location before encrypting it on the hard drive. Hard drives often don't fail completely but will fail slowly, a few sectors at a time, getting worse and showing more symptoms as they fail.

Support issues (Continued)

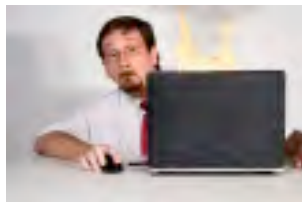
The process of encryption may push a borderline hard drive, which previously showed few symptoms, over the edge.

The encryption process, which begins about five minutes after login (following restart required by the software install) takes from four to eight (or more) hours depending on certain computer characteristics such as hard drive size and processor speed.

Support issues (Continued)

The hard drive is working constantly during this period of time and every sector is accessed. This is probably more use than the average hard drive normally sees.

Support issues (End of a Hard Drive)



User Training

There is very little user impact resulting from the Disk Security software. The big difference people will experience is the log-in process.

User Training (Continued)

There is an extra step called pre-boot authentication before the operating system is loaded.



◀ **boot**

User Training (Continued)

The Disk Security user account can be set up to mirror the user's local workstation account and the password can be set to synchronize with the Windows account. This works well.

User Training (Continued)

After a "password change successful" message, the user will receive a message from Pointsec that the Pointsec for PC password was changed successfully.

Problems which have been reported regarding passwords have not increased significantly.

User Training (Continued)

However, when a password has to be reset there are a few extra steps involved to get everything synchronized again.



User Training (Continued)

The Media Security software has a steeper learning curve for the users though. There are procedures for encrypting data that is stored on various types of removable devices.



User Training (Continued)



Procedures for sharing this data with <other computers that have Media Security software installed> vary with those for sharing it with <computers that do not have Media Security>.

User Training (Continued)

There are several different types of passwords that can be set by the user.

User Training (Continued)

A password can be set for the software installation on the computer, for each individual removable device that is attached, and passwords can also be set for each encrypted package that the user creates.



User Training (Continued)

Some users will be intimidated by all of these options, so it is necessary to provide instructions on what to do, as well as provide departmental policy on what is required.



Some Final Notes



To sum up our experience with Entrust, we have to say it has taken some time to get the hang of this software.

Not just how to use it but how to install and administer it also.

Some Final Notes (Continued)

This has not happened without some glitches and frustration ...



Some Final Notes (Continued)



... but even though the process of encryption requires a few extra steps, the assurance that sensitive data is protected makes this worthwhile.

Some Final Notes (Continued)

We were able to take the product that Entrust offered and utilize it for the specific needs of our department. Overall, we believe Entrust offers a solid solution for protecting sensitive data and that the Entrust support team is readily available when assistance is required.

Final Note

We have not received any incentives from Entrust to make this presentation.

This presentation has not been shared with anybody from Entrust.

We are simply sharing the positive experience we have had with the “solution provider” we chose.



Any Questions?

Come Visit Us in Tennessee!

