

Customer Profile

Large government department

RSA SecurID® aids highly-secure remote hard drive encryption

Acceleration

“The RSA SecurID 800 hybrid authenticator was pivotal in enabling us to accelerate the rollout of hard drive encryption to our laptop users from many months to just eight weeks. What's more, by deploying encryption remotely we were able to keep costs down and reach 95 percent of the devices in one hit.”

Risk Director

AT A GLANCE

Business challenge

- Further improve the security of sensitive data, including Personally Identifiable Information
- Deploy government-approved hard drive encryption to 10,000 laptop users, with no remote management functionality

Solution

- RSA SecurID 800 hybrid authenticator pre-loaded with a serial key kicked-off remote rollout
- Authenticator then replaces existing hardware token for strong authentication for remote access to systems

Results

- Full deployment took just eight weeks and achieved 95 percent saturation for a minimal cost and minimal inconvenience to the end-user
- No one individual was exposed to more than one key rollout stage, assuring high security in line with government guidelines

This government department ensures that the correct tax is paid at the right time, whether this relates to payment of taxes received by the department or entitlement to benefits paid.

BUSINESS CHALLENGE



Over the past decade, the media have successfully raised consumer awareness of data privacy. Nowadays, data security breaches have a negative impact on organisations, as well as their customers. Losing confidential information can result in adverse press coverage, lack of consumer confidence or even legal penalties.



With this in mind, this country's Government set up a service that enables private sector companies to develop cryptographic products to approved standards for use by the Government and other appropriate organisations.



By its very nature, the government department responsible for tax holds a

lot of sensitive Personally Identifiable Information (PII), therefore ensuring data security within this department is critical. For this reason, it tasked its IT outsourcer with deploying hard drive encryption to 10,000 laptop users.



The Security Division of EMC



SOLUTION

One method for deployment was to set up secure, temporary remote offices where users could bring their laptop for encryption. But installation takes four hours per device, so the department would have needed 40 offices, with 1,000 staff and a two-month set-up period.

Additionally, it would have been difficult to persuade people to travel to one of the new 40 sites, increasing the probability of missed or cancelled appointments. An estimated 20 percent dropout rate would have extended the rollout period to many months. This was too lengthy, costly and unreliable.

Instead, the IT outsourcer formulated an ingenious alternative. From a secure management centre staffed by 40 people using the department's internal post, it sent an RSA SecurID 800 hybrid authenticator pre-loaded with a serial key to each user, asking them to email a central clearing house to confirm receipt. It then used the department's regular HP Radia remote management tool to push B-Crypt out to the laptops, without installing it.

A separate team of 120 agents in another secure location then sent the users an email, asking them to confirm a date, time and location where they would be with their laptop connected to the LAN. From here, the user phoned a central number where they were connected to one of the agents. The agent then matched the caller's ID number to the allocated authenticator serial number.

After asking them to log in, the agent then logged on remotely as the local admin using CA Unicenter systems management, and asked the user to plug the authenticator into the USB port. The agent then entered an installation password from their database that generated a temporary password, which they told the user over the phone. They then logged out and rebooted the machine, moving installation to the next level. The user then logged back in and entered the temporary password to begin the full encryption.

RESULTS

Using this method, full deployment took just eight weeks and achieved 95 percent saturation. A team was on hand to fix a number of problems locally, but these were minimal.

Despite the initial rules, the outsourcer found a way to deploy hard drive encryption remotely, and still in line with Government-approved guidelines. Three factors enabled it to achieve this highly-secure, remote rollout. Firstly, the key used to encrypt the hardware was only seen by 40 agents. Secondly, the initial installation password was only seen by 120 (different) agents. Finally, the end-user password was only seen by the end-user. As a result, no one individual was exposed to more than one key rollout stage.

The users then replaced their existing RSA SecurID hardware token for remote system access with the new RSA SecurID 800 hybrid authenticator. This two-factor authentication solution verifies something the user knows - a password or PIN, as well as something the user has - a six-digit code that changes every 60 seconds. The SecurID 800 authenticator can also store certificates and Windows domain passwords, providing a more convenient and reliable level of user authentication than reusable passwords.



"Despite initial rules we found a way to deploy hard drive encryption remotely to laptop users using RSA SecurID. Not only did we achieve this in line with government guidelines, it was also done for minimal cost and with minimal inconvenience to the end-user."

Risk Director



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

RSA, the RSA logo, SecurWorld and SecurID are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the property of their respective owners. ©2003-2007 RSA Security Inc. All rights reserved.

GOVDEPT_CP_0909