Secure Access to the GCSx: Achieving CoCo Compliance

Government employees can now safely connect to the GCSx and share “sensitive personal data” with other local and central governments. By using strong dynamic passwords, identity theft and data leakage can be prevented.

COCO: SIMPLIFYING AND SECURING INFORMATION FLOWS

Obtaining sensitive personal data of citizens needs to remain easy for government employees. However, it must remain secure from hackers and fraudsters. Therefore Government Connect enforces the usage of the Government Connect Secure extranet (GCSx) when exchanging sensitive information. By centralizing the information on the extranet, the public sector can benefit from this secured communication channel. It can improve reputation and gain public confidence and enhance citizen centric services.

Besides exchanging sensitive information on a common platform, GCSx allows you to securely access applications and exchange emails. By storing information at a central location, the data doesn’t need to be sent over the internet or by post, making them less vulnerable for interception. Information can now be shared by the right people in an instant.

OBTAINING COCO COMPLIANCE

CoCo compliance is obtained when local authorities comply with the list of security requirements. These requirements prescribe the following criteria need to be met:

- Secure mobile access to government applications
- Enhanced user authentication and controlled public access
- Enforce the usage of more complex passwords

By implementing a strong two-factor authentication solution based on dynamic, one-time passwords, the CoCo security requirements can be met. Dynamic passwords are generated by a DIGIPASS®, that generates a unique code every 32 seconds. This code is then used in combination with your username and/or PIN code whenever you need to logon remotely or enter a government application.

- In March 2008 there were 76.8 million National Insurance numbers in the UK, with a population of 61 million.
- 77,500 cases of identity and impersonation fraud were reported in 2007, UK only.

http://www.cifas.org.uk
The fact of combining something you know (a username or a PIN code) with something you have (a One-Time Password generator), is what is called in industry terms: strong user authentication, which is what the CoCo criteria stipulate.

Remembering complex passwords is no longer needed, with one push on the button on the DIGIPASS device, you receive a unique code that will allow you to access your applications regardless of the place where you are working from. This unique code can only be used once and is valid for a limited period in time, thus preventing identity theft and data leakage.

STRONG AUTHENTICATION SOLUTION BENEFITS
- Complies with the most stringent government standards
- Seamlessly works over any network and traverses any firewall
- Access to web, applications, and to files from a single solution
- Significant savings in user costs because deployment isn’t necessary
- Total solution at a competitive TCO & ROI

For more information: www.vasco.com

MULTIPLE CLIENT DEVICES:
- Smart Card
- Card Reader
- DIGIPASS device
- OTP generator
- e-Signature generator
- Mobile phone
- Pocket PC
- Laptop
- …

MULTIPLE SERVICES:
- Identity Management
- Fraud detection & Analysis
- Statistics & Reporting
- VPN
- Consulting
- Fulfillment
- Device personalization
- Support and Maintenance
- …

MULTIPLE APPLICATIONS:
- e-Banking
- e-Commerce
- e-Gaming
- e-Insurance
- e-Government
- Healthcare
- Education
- Automotive
- …

About VASCO

VASCO designs, develops, markets and supports patented DIGIPASS®, DIGIPASS PLUS, VACMAN®, IDENTIKEY® and aXsGUARD® authentication products for the financial world, remote access, e-business and e-commerce. With tens of millions of products sold, VASCO has established itself as the world leader in Strong User Authentication for e-Banking and Enterprise Security for blue-chip corporations and governments worldwide.

www.vasco.com

Copyright © 2009 VASCO Data Security, Inc. VASCO Data Security International GmbH. All rights reserved. VASCO®, Vacman®, IDENTIKEY®, aXsGUARD®, DIGIPASS® and ® logo are registered or unregistered trademarks of VASCO Data Security, Inc. and/or VASCO Data Security International GmbH in the U.S. and other countries. VASCO Data Security, Inc. and/or VASCO Data Security International GmbH own or are licensed under all title, rights and interest in VASCO Products, updates and upgrades thereof, including copyrights, patent rights, trade secret rights, mask work rights, database rights and all other intellectual and industrial property rights in the U.S. and other countries. Microsoft and Windows are trademarks or registered trademarks of Microsoft Corporation. Other names may be trademarks of their respective owners.