

United Kingdom (UK) Government Connect Secure Extranet (GCSx) Code of Connection (CoCo)

Using Apani® EpiForce® Logical Security Zones and Encryption as
a Regulatory Compliance Solution and Local Authority Best Practice



Introduction

This paper addresses the challenge of key regulatory compliance requirements driven by the GCSx CoCo. As this paper suggests, the best response is to take a risk-based approach that builds on a base of server isolation and end-to-end encryption to separate the local authority network from the GCSx network and control user network access.

What is GCSx CoCo?

Government Connect (GC) is UK government program led by the Department Works Project (DWP) that established a secure communications network for English and Welsh local authorities. The pan-government, private wide area network (WAN) is called the Government Connect Secure Extranet (GCSx) or GSX in Scotland. Its purpose is to support improved cooperation between the government and local authorities. Through March 2011, the GCSx has a £33m funding package to complete its delivery and operation. Starting in April 2009, GC will begin to replace current vulnerable internet- and postal-based solutions with GCSx.

On 31st March 2009 DWP will cease the provision of RESTRICTED data to local authorities and the receipt of sensitive personal data from local authorities through means other than government approved secure communications channels. GC is targeting English and Welsh local authority connectivity by that date. To deliver protected electronic services to the public and meet the deadlines, local authorities should have already started the application process. To be approved to connect to GCSx, local authorities need to sign up to the Code of Connection (CoCo) that defines the minimum security standards and procedures with which an authority must comply.

The approval process takes time and there are important steps authorities must take to achieve compliance, such as submitting a compliance statement and supporting information that the authority has adhered to CoCo security control measures. Each local authority is assigned a regional account manager to assist it in the compliance process. Local authorities should refer to the GC website <http://www.govconnect.gov.uk> for more information on GCSx CoCo and to contact the regional account manager.

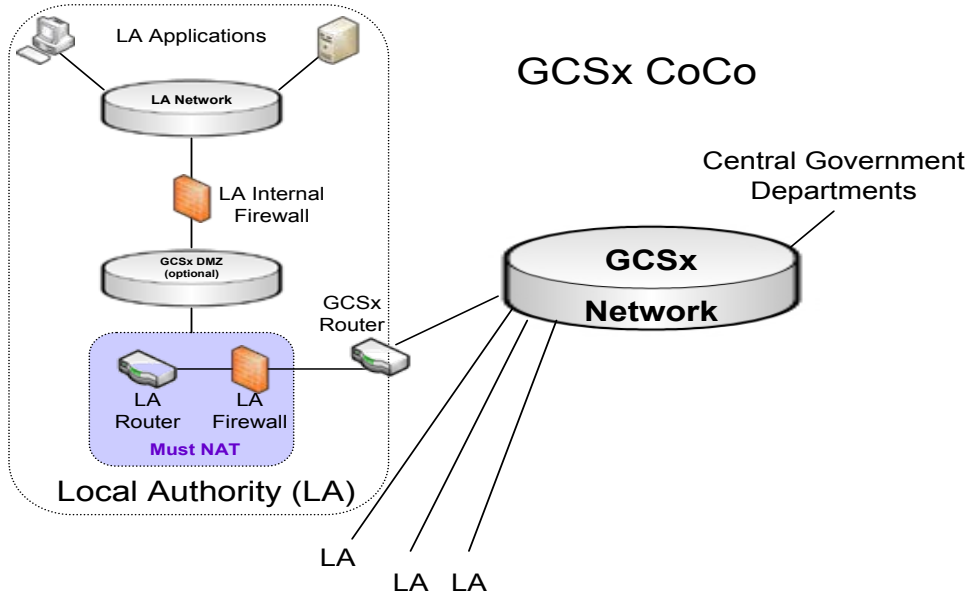
What are Key Security Challenges in Complying with the CoCo?

The CoCo consists of over two dozen assessment controls related to data and network security. The focus of these controls is to require local authorities to mitigate the risk of a security breach and strive to prevent access to data and networks that carry sensitive data. A local authority may implement a different approach than another authority if that approach is deemed acceptable by the GC Assessment Team in mitigating a security risk.

It is also clear that many different security solutions and processes are required to meet the many CoCo compliance requirements. For a complete list of the CoCo, local authorities should contact the GC. GC regional managers are available to assist local authorities in implementing what is required to meet the CoCo.

Limiting the Scope of a CoCo Audit

The diagram below depicts what authorities should do locally to protect their communication to the GCSx. As you can see, internal firewalls and optionally setting up a GCSx DMZ are recommended approaches.



Source: <http://www.govconnect.gov.uk/what-is-gcsx.php>

The larger the network and the more critical data is dispersed, the more complex and time consuming an audit will be. Local authority networks are typically large and flat structures which contribute to this challenge.

Deploying internal firewalls and routers is a way to segment a flat authority network to limit access to critical data. The problem with traditional hardware segmentation is that it puts some limits on resource sharing capabilities and is difficult to modify once established. The process of adding new zones, devices and users is often hard to document and difficult to audit.

More importantly, hardware segmentation cannot effectively segment based on application and does not allow a single device to be present in more than one segment. Firewalls were designed as perimeter protection devices and installing them inside the perimeter can often cause more headaches than solutions. Managing firewalls through Access Control Lists (ACLs) is a difficult, time consuming feat of endurance. Opening a port for one application and then failing to close the port later when the application is no longer in use, creates a serious security liability

Controlling Remote Employee, Public and Third-Party Access

Local authorities often have remote employees with authority or private laptops, public reception areas where customers can self-serve (complete an application form, sign it and apply for benefit electronically) and third-parties or contractors that need access to resources on the network. Controlling access by these users and systems to hosts with critical data presents a difficult challenge. GC assessors will need to determine that these access points are managed by the local authority as part of the “untrusted” network, with no direct access to the local authority network.

Many companies use network firewalls and access control lists to physically separate users. While this may be acceptable for small authorities with limited types of user access, large authorities often have a variety of user access from multiple locations simultaneously. This type of deployment makes firewalls difficult to deploy and maintain. Once inside the corporate network, remote employees, public and third-party access can improperly gain access resources, increasing the risk of a data breach.

Protecting the Private Authority Network

The GCSx CoCo requires that data at rest and in transit be encrypted to protect information traveling over open, public networks. Critical information is scattered across the private network

and is often in transit. Most authority internal network data traffic is generally sent in the clear and that traffic is vulnerable to a packet sniffer used by an “untrusted” user. In other industries, such as financial services and retail, data thieves have shifted their focus on targeting private network data.

Although GCSx CoCo does not require encrypting data over private networks, authorities should explore ways to reduce the risk of an internal breach. One way to mitigate the risk of an internal breach is to encrypt data on internal networks.

Implementing Virtualization Security

Virtual machines (VMs) themselves are no less secure than physical systems, but authorities often apply different procedures to their deployment and management creating vulnerabilities. Legacy security solutions such as firewalls function outside the host requiring new tools to isolate and protect critical data inside the host. Also firewalls require associating an IP address to a location and making a security decision based on that location.

In a virtualized environment, during VM migration, IP addresses often change as virtual machines are created, retired or migrated from one physical host to another, causing issues in traditional protection mechanisms. Finally, VMs are easily created from previously existing images, often introducing large numbers of VMs, also known as VM sprawl, that are not properly maintained or are based on images with known vulnerabilities.

Apani EpiForce Assists with CoCo Compliance

Most local authorities are aware of the need to secure their critical systems from unauthorized access but there remains a large portion of systems on the network that are often unprotected or trail behind in security standards, such as those that are used for internal local authority use. Additionally, internal network communications pose a big threat for potential security breaches as they are usually “open” systems and are easy targets for hackers and data theft.

EpiForce Logical Security Zones

EpiForce logical security zones offer a superior, software-based alternative to traditional network segmentation accomplished through network firewalls. EpiForce zones enable large, flat authority networks to be separated into isolated security communities without reconfiguring the network and without regard to physical location of computers. Computers or users are assigned membership into one or more logical security zones, creating a flexible, layered security approach within the corporate network. Once implemented, EpiForce zones protect authority networks from vulnerable systems, isolate critical data to need-to-know employees, isolate third-parties to appropriate systems and these zones are transparent to applications and infrastructure.

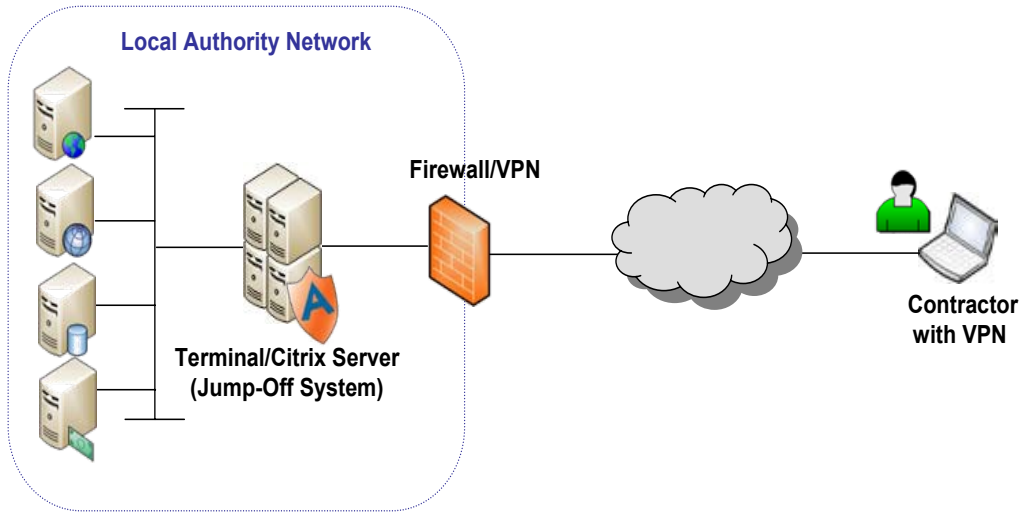
EpiForce Third-Party Isolation

As shown in the diagram below, EpiForce third-party or contractor isolation utilizes logical zones to enable movement of remote employees, public and third party user access without losing policy.



EpiForce is transparent to leading VPNs and applications. In a scenario involving Citrix/Terminal services, multiple users are logged on to a Citrix server at the same time; each User receives a policy specific to their User ID and applicable Zones. EpiForce supports a “location-based” policy where the same machine or user has different policies applied based on their location as defined by their IP address. Finally, EpiForce supports “hot desking” where two or more people are using the same machine one at a time receive different policies based on their User ID.

In the picture below, EpiForce preventive jump-off works to control access of remote users to the private network to deliver secure third-party isolation. A third-party who could be from any of several firms has a need to access specific resources on the authority network. This third-party user may have limited access to systems or full administration rights. The user via a VPN communicates over the Internet through the firewall VPN appliance guarding the corporate network. The appliance terminates the VPN, authenticates the remote user, provides an IP address from a pool and controls the destination the remote user can connect.



In this case, the remote user is directed to a terminal server or Citrix server with the EpiForce Agent installed. Based on remote user policies, the agent blocks server ports, runs multiple interactive shells (e.g. telnet, FTP, RDP, SSH). For example, the jump-off server can allow port 21, block port 80 and allow port 189. Therefore, a single EpiForce Agent can efficiently control multiple remote users and their security policies and mitigate the risk of an unauthorized access to critical data.

EpiForce Policy-Based Encryption

Best practices for protecting critical data is end-to-end encryption, which is not required by CoCo. EpiForce manages the encryption of critical network traffic. A security policy would be created that encrypts the critical data in motion from traveling on the network. An encryption policy may also be created to direct that only the TCP ports that transmit critical are encrypted. A policy can also be defined to isolate the critical data environment away from the rest of the network allowing only network connections into the environment from hosts that the local authority fully trusts.

EpiForce Virtualization Security

For local authorities deploying server virtualization, EpiForce is an ideal security solution. Once an EpiForce Agent is installed on a virtual machine (VM), the VM can be assigned to a PCI security zone regardless of where the host or VM is located. Multiple VMs in that host or other hosts in different locations can be assigned to security zones, to deliver efficient use of IT assets.

EpiForce manages both virtual and physical IT assets, regardless of platform or physical location. Deploying a virtual-only security solution requires authorities to take a silo approach to security, increasing management complexity. EpiForce alleviates this concern by managing both virtual and physical servers and clients from a centralized console.

Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or endpoint. When a VM is created and/or moved using VMotion or Virtual Center, the security policy goes with the machine and does not require any policy changes or administrative action. When EpiForce VM is deployed, agents also automatically reconfigure security policy when a VM is restarted, avoiding a security gap.

Apani EpiForce: Benefit Summary

UK local authorities are faced with the challenge of complying with the key regulatory compliance requirements driven by the GCSx CoCo. The best response is to take a risk-based approach that builds on a base of Apani EpiForce server isolation and end-to-end encryption to separate the local authority network from the GCSx network and control user network access. EpiForce delivers:

- Logical security zones to protect local authority networks from vulnerable systems, isolate critical data to need-to-know employees, isolate third-parties to appropriate systems in these zones
- Preventive jump-off to control access of remote users to the private network to deliver secure third-party isolation.
- A reduced risk of an internal data breach through policy-based, end-to-end encryption
- Security for virtual machine, physical servers and clients from a centralized console to reduce management complexity

EpiForce is easy to deploy, highly scalable and transparent to infrastructure, applications and users, and it will meet the needs of any large authority. For a free GCSx CoCo assessment and how EpiForce can help, call Apani Europe at +44 (0) 207-887-6060.

About Apani

Designed to isolate servers, VMs, endpoints and business-critical data within the corporate network, Apani EpiForce VM is an ideal solution for flexible access management and is trusted by the world's largest financial service organizations. More than 60 Fortune 100 companies use Apani's core technology, which was created with a grant from the National Security Agency to protect communications in the event of a nuclear war.

By isolating systems into logical security zones and strictly controlling who has access to these security zones, EpiForce is a superior alternative to deploying, configuring and managing firewalls and VLANs.

Due to its software-based architecture, EpiForce is easier to manage, more flexible, quicker to deploy and has an overall lower total cost of ownership. Leveraging digital certificates to authenticate users and systems, EpiForce strengthens authentication in virtual environments.

EpiForce is easy to deploy, highly scalable and transparent to infrastructure, applications and users, and it will meet the needs of any large corporation.

For more information on Apani or EpiForce, visit www.apani.com.

08-026 12/08