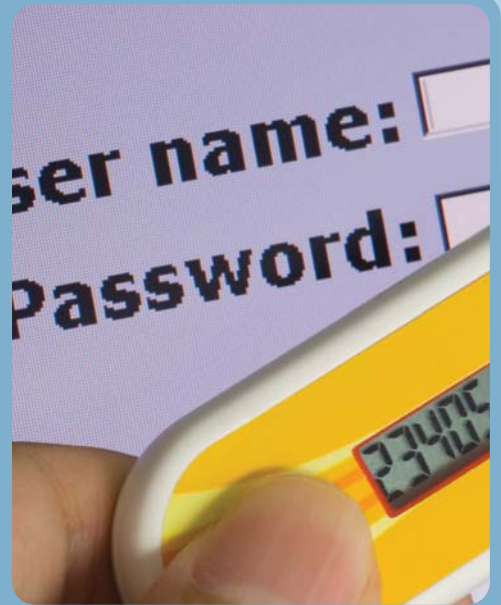


# Do Local Authorities need to beef up their security? *I should CoCo!*

Paul Lewis, Network Consultant



An important deadline is looming for Local Authorities. The Government is requiring them all to connect to the Government Connect Secure Extranet or GCSx network, which has its very own Code of Connection or CoCo. The deadline for signing up as compliant to the various security control measures it contains is **31st March 2009**.

## What is the GCSx?

The GCSx is a Wide Area Network (WAN) provided by Cable & Wireless, under contract to the Government. The aim is to provide robust and secure inter-connection for the networks of Local Authorities, critical Government bodies, and other approved organisations.

GCSx, for instance, provides secure gateways to the NHS (N3), the Government Secure Extranet (GSX), the Criminal Justice Extranet (CJX) and the Police National Network (PNN).

Critically, the GCSx and interconnected networks are approved to carry sensitive information, such as personal data and that classed as restricted. This will help bodies adhere to their duties under the Data Protection Act.

As a single network, from a single vendor, it should also be much easier to define and monitor Service Levels on the platform, which is not the case with most Internet-based connectivity, even when it is adequately secured (for example using encrypted IPSec tunnels).

## What are the key compliance requirements?

There are lots of requirements covering all areas of ICT security, though some are recommended rather than mandatory. One of the main stumbling blocks affecting Authorities is the mandate that remote workers accessing the networks must authenticate strongly, using a two-factor process.

## What is Two-Factor Authentication?

Authentication is the process of confirming that someone is who they claim to be. Two-factor

authentication insists that a user requiring a service (in this case, remote connection to the network) provides two different pieces of verifiable evidence concerning their identity:

**Something they know** - usually a passcode or PIN  
**Something they have** - this is usually a small token device, though these days there are a number of alternatives, including biometrics (almost what they are, rather than what they have!)

The key idea is that, if just one of the criteria is compromised (for example a token is lost, or someone has obtained a password or PIN by social engineering), access security is not compromised.

If you think about it, this is a process we all know - and mostly trust - for accessing our money through a cashpoint - you're stuck without both your bankcard and its PIN.

In IT terms, two-factor authentication has been around for a long time, but it has not been implemented by many organisations despite the proven security benefits; primarily because of cost. Many organisations are now starting to realise that these costs are, relatively speaking much lower, as the same system can now be used to authenticate multiple services, including IEEE 802.1x Wired and Wireless LAN authentication, Dial-up, IPSec and Secure Sockets Layer (SSL) VPN network access. Strong authentication is also proving invaluable for securing management access to key IT systems such as server, switch and firewall administrator logins.

Far and away the leading vendor for two-factor authentication systems is RSA Security (now a division of storage giant, EMC) - in fact RSA's pedigree in the Security arena means that virtually all systems incorporating encryption technologies for instance, are underpinned by RSA technology.

## RSA Authentication Manager and SecurID authenticators

RSA's system is based around its Authentication Manager (formerly known as ACE/Server). This acts as the central two-factor authentication system to which points of network access, such as VPN concentrators, Firewalls or Wireless Access

Points, are referred when receiving connection requests. Traditional hardware tokens, such as those commonly seen on key-rings, are still the most popular authenticator. However, increasing use is now being made of newer alternatives including software on smart-phones or PDAs, which does the same job, without requiring a dedicated device.

In addition to its two-factor capabilities, Authentication Manager also incorporates the widely deployed and proven Steel-Belted RADIUS software. RADIUS (Remote Authentication Dial In User Service) software is often an intermediate port-of-call for remote access authentication, before referral to a two-factor authentication system - providing additional authorisation and accounting features. This means that the full deployment requirements for secure remote access can be delivered with a single solution.

Another relatively recent RSA development is the availability of Authentication Manager in a dedicated, hardened appliance format, making it simpler and easier to deploy and maintain.

RSA has understood the challenges Councils face in meeting CoCo requirements and have responded with special pricing for two-factor authentication services, in this vertical space, available until the CoCo deadline at the end of March.

## How Networks First can help

In addition to our proven skills in core aspects of networking, we have a long history of working with RSA's SecurID 2-factor authentication system. Not only can Networks First help advise Authorities in choosing the right blend of authenticators for their users' needs, but can also provide fully managed deployments, including the key role of integrating the system with numerous access technologies from many different vendors, including Cisco and Check Point. We can also, of course, provide tailored and responsive support services to keep the network and its security system working into the future.