

Visit our website for local government authorities [www.cryptocard.com/locgovt](http://www.cryptocard.com/locgovt)

### Why councils have already chosen CRYPTOCARD

**Hampshire County Council** wanted to get ahead with their compliance. "We decided we needed to act now to ensure the system was fully operational before the Code of Connection deadline arrived. Our needs were clear; a 2FA solution that met the CoCo requirements, was within our budget and was easy to install and deploy to our workers." Jane Stedman

**Lewisham County Council** were looking for a solution that allowed local government workers to have required access to their system whilst enabling their own workers to have access from not only the central office but also if working with other agencies.

**Rotherham Council** wanted to improve productivity and work/life balance for its employees by enabling them to work from home or other locations outside of the office. They required a secure, cost-effective solution and to have it fully implemented quickly.

The **Isle of Wight Council** has been a CRYPTOCARD customer for many years. It deployed the CRYPTO-Shield server in 2001 and used it to secure remote access for over 200 workers. However, the Code of Connection meant that whilst reviewing their policies and looking for areas to reduce capital expenditure, they engaged CRYPTOCARD to assess the managed service which offers the same, high level of security but allows additional flexibility without requiring a server

**Cornwall Council** has been looking at where it can make financial improvements becoming a unitary council. To enhance their collaborative working across its unitaries and to comply with the Code of Connection, Cornwall secured its access for its remote workers by deploying CRYPTOCARD.

**North Somerset** assessed the CRYPTOCARD solution as part of their assessment for the Code of Connection. It was the most cost effective and flexible with easy deployment.

**East Lindsey Council** wanted to add additional functionality to its existing CRYPTO-Shield server to allow secure access to web mail and remote access network as part of their Code of Connection compliance.

**Lancaster City Council** found CRYPTOCARD "extremely cost effective whilst being easy to deploy." As a result they are looking to roll it out to other business areas to enhance security protocols.



## A guide to secure, complex passwords for the Code of Connection



### CRYPTOCARD solutions:

- ✓ Meet Code of Connection criteria
- ✓ Allow you to set your IT Policy
- ✓ Integrate into existing network structure
- ✓ Work across multiple platforms
- ✓ Offer a full range of tokens that can all operate on same system
- ✓ Long lasting tokens with replaceable batteries
- ✓ Server-based or managed service solutions
- ✓ Lowest total cost of ownership in the industry

### CRYPTOCARD Europe

Eden Park, Ham Green  
Bristol  
BS20 0EB UK

Tel: +44 870 7077 700  
Fax: +44 870 7077 711

E-mail: [info@cryptocard.com](mailto:info@cryptocard.com)  
[www.cryptocard.com](http://www.cryptocard.com)

Understand why Authentication is an important part of Government Connection GSCx and what this means for your public sector organisation

## This guide will explain:

1. What the CoCo criteria stipulates for passwords
2. What two-factor authentication is and how it works
3. Why hackers hate 2FA
4. How to secure your remote access and systems
5. How councils have benefited from 2FA

## Code of Connection criteria

CESG Memos 26 & 35 sent to all authorities. Actually states that password complexity must cover the following criteria:

1. Must contain a minimum of 7 characters
2. Must be alphanumeric with at least 1 numeric
3. Must be changed at least every 90 days
4. Cannot reuse the last 20 passwords
5. Cannot use any part of the users assigned account name
6. Must not be shared or written down

The Government Connection and the GCSx (secure Extranet) is about to have an impact on the way in which you and your staff work.

Although this will be a major benefit, putting the correct policies in place to deliver better flexible working and the stronger security measures that mean systems are better protected and identity of users accessing data is assured will also require greater IT administration and help desk headaches.

We've put this simple guide together to assist every council that is at stage 2 of the process - Reviewing and Consulting - or stage 3 - Completing the Assessment. (If you are still amongst the authorities that are at stage 1, keep this document close to hand to assist you later on).

### Connection is key

Remote workers and flexible working is becoming a standardised practice as organisations take advantage of cost benefits of the internet by providing VPN's (Virtual Private Networks) for employees to access confidential corporate data, resources and protected applications. Users at all levels now have the ability to access systems from home, other offices or remote locations such as hotels, café's, etc.

Whilst VPN's protect the integrity of the data's transmission verification that the user is who they say they are is reliant on a single static password that can be lost, stolen, shared or easily guessed - however complex it is made.

### What this actually means

The criteria set is excellent for keeping your system secure and provides a useful check list for councils when assessing the options. However, you may want understand what the reality of the risks are.

CRYPTOCARD's VP Europe, Jason Hart, was an Ethical Hacker who tested systems for security vulnerabilities and therefore knows only too well the damage that can be done by unauthorised access to a system by a hacker.

"Hackers have the ability to deface, damage or steal data once inside a system. They look for easy ways into it, often by obtaining a static password. Social networking websites, such as Facebook, have unfortunately, helped hackers find static passwords as many people use passwords that are personal to them- such as their children's names, favourite football team or a pet's name. If not, the 'brute force' method with software that tries thousands of words per minute is another way to 'crack' the correct code - even including complex alphanumeric passwords.

"Remote access is most vulnerable because 'password sniffers' use software that capture the password at the time that it is used. So, if you are sitting in a hotel or airport lounge logging on to your network via your laptop, the man sitting across from you could be downloading your login details and much more.

"Even VPN's are not completely secure for this reason. As standard, there is only the static password which is rarely or perhaps only periodically changed to protect it.

"It may seem that regular changes to the password is the crucial element to securing your system but we need to also remember that most humans are terrible at remembering combinations! How many telephone numbers do you know 'off the top of your head?' And it becomes an impossible task when meaningless or random combinations are used. How can you ensure a user remembers X3y8g4tU?

"We also tend to have several passwords to remember any way - between your personal email, bank login and online shopping accounts - most people have about 20 passwords to remember.

"This is where user would fail in the system. They either write it down or use the same one for everything (which breaks criteria 6 and becomes a security risk on its own) or forget it and has to get it reset by the IT helpdesk with resource costs to consider.

"In 2007 hackers were able to gain access to the TKMaxx computer systems and see unencrypted credit card data as the information was processed from their stores' till to the banking network. They were also able to see customers' addresses and other information that could allow them to commit identity theft.

"This is why I, and other ethical hackers, strongly recommend two-factor or dual authentication and the use of one-time passwords."

### But how can an IT department enforce that this criteria is adhered to?

This is where two-factor authentication (2FA) provides a simple answer. It ensures that the account user is who they say they are as the login process requires a couple of pieces of information to match before allowing access to systems in a similar way that to your bank card.

There is something that you 'know,' such as your 4 digit PIN, and something that you 'have,' this is known as a token and provides a one-time password which is never repeated. It goes without saying that the more complicated, the most secure this is. The most secure is Base 64 which is a binary string of data that uses alpha (upper and lower case) and numeric random strings of 8 digits.

The password is impossible to share and would be pointless at writing down (it would be invalid once used).

A good authentication system gives you the flexibility to provide the users with the most appropriate form of token too. For example, you may have office based workers who will require desktop access to certain systems whilst other may work remotely and require a physical device that allows secure login from another computer without the threat of passwords being copied and re-used. Also, beware of some forms of authentication that require a response - where the same response string is returned each time (e.g. the 2nd, 4th, 6th and 8th character is the response) as once intercepted, the hacker will only need to gain the next string to access the system.

An organisation is also going to need flexibility when it comes to integration. Code of Connection doesn't solely revolve around authentication. Firewalls and Intrusion prevention, detection scanning and anti virus tools will be part of the package and so simple integration of your 2FA should be high on your agenda.

### What will I need to purchase?

This will depend on the resource available and also whether you would prefer to invest in a server or 'buy-in' the server on a per user basis. We have a simple decision tree available to help you make this decision on our Code of Connection microsite.

Visit [www.cryptocard.com/locgovt](http://www.cryptocard.com/locgovt) to find out more.



Some of the questions you need to consider when securing your remote access:

- How many remote workers are there?
- How are they going to gain access? Via a VPN? Via Citrix?
- What devices will they use? Laptops? Home computers? Blackberry devices?
- Who uses web mail?
- Do you need to provide users with access to any web based applications?
- Do you use wireless networks?
- How will you allow 3rd parties access to specific areas of the network? e.g. suppliers or other authorities

Below are some of the key differences and requirements of the 2FA options available:

**Server** - The organisation installs the server in-house and takes responsibility for installation, deployment and management of it. If you require the authentication on a platform other than Windows check it will allow you to do this. You will want to consider a replica server and you should also look at what management reporting is available. Look for hidden costs too - for instance licences can vary with hidden costs as they require renewals. A good guide to your investment is to work out the total cost of ownership which includes upfront costs and ongoing costs that are required - some solutions can be considerably more expensive when worked out over a 5 year period.

**Managed Service** - The organisation doesn't need to make upfront investment and requires no infrastructure from an outsourced authentication. It should be simple to use and be flexible for administrators to effect organisational changes as and when they occur. As it works by acting "sitting in front" of your network and only allowing access to those with the correct credentials it's got to be reliable and is ready to offer support should an issue occur.

**Tokens** - You will probably have a different groups of users and will therefore require the most cost effective token for their needs. Consider how often will the need to login and how vulnerable their access is (e.g. will they only logon to their own desktop or might they be using other computers to do so?)