

© Oxford Computer Group
Overview document



Government Connect Code of Connection

"Some Issues to Consider and the Technologies at Play"

UK Public Sector

Version 0.1.1
Wednesday, June 24, 2009

Oxford Computer Group
Proprietary & Confidential

www.oxfordcomputergroup.com

Overview document for UK Public
Sector
Government Connect Code of
Connection

Tel: +44 (0)8456 584425

Contents

Meeting the Code of Connection.....	3
The Business Challenge	3
Secure Remote Access Control.....	3
SSL VPN – Browser-Based Remote Access.....	4
Data Integrity	4
Application Manipulation.....	5
User Experience	5
Two-factor Authentication with One-Time Passwords	5
Hard Tokens.....	6
Soft Tokens	6
Clientless Authentication	7
Conclusion.....	7

Meeting the Code of Connection

Secure Remote Access and Two-factor Authentication

The Government Connect Code of Connection (CoCo) is designed to deliver many key commercial and operational benefits to local and regional government bodies. These benefits include:

- Improving inter-government communication.
- Creating faster, lower cost interaction between organisations and the public.
- Enhancing client services.
- Defining a standardised means of securing access to resources, systems and communications.

In this brief document we explore some of the issues to consider before you implement a solution and explain some of the technologies at play. We also provide links to places where you can obtain further information.

The Business Challenge

At some point it will become necessary for all government organisations to become compliant with the Government Connect Code of Connection. However, there is no one way to achieve this and the challenge is therefore to find the most appropriate route for your organisation and technology landscape without introducing too many different vendors and solutions. This means ensuring that the right mix of products is deployed to cover the different facets of the code without introducing unnecessary complexity and the increased costs of managing a multi-vendor infrastructure.

Secure Remote Access Control

One of the Code of Connection 'Challenge Areas' relates specifically to remote access and how to control access from devices that are not owned or specifically managed by the local authority. This challenge area also refers to two-factor authentication and encryption.

The CoCo FAQ document states that when providing remote access to home and mobile workers, local authorities must provide a CoCo compliant solution for mobile working and this must include two-factor authentication.

So what is the best way to meet this specific aspect of the Code? Is it possible to deploy a solution that allows you to provide enhanced access and communication whilst also providing it in a simple and integrated manner? And what about complexity? Does a secure remote access solution require

solutions from multiple vendors and if so, how easy is this to manage?

SSL VPN – Browser-Based Remote Access

The most common mechanism of providing remote access is a Secure Sockets Layer (SSL) Virtual Private Network (VPN). This is an ideal platform for meeting aspects of the Code of Connection because it can provide browser-based access to corporate resources. This means that resources can be made available to the broadest possible audience, regardless of their IT skills or familiarity with technology.

By using the browser rather than a VPN client to access resources the following benefits can be attained:

- No need to deploy VPN clients and train users
- Reduced deployment and management costs
- Faster provisioning and de-provisioning of the service
- Reduced helpdesk costs

Because a VPN client is not present, access control is delivered through user-based policies at the SSL VPN gateway. It is these policies that control and limit access, only granting access to the resources that a user's profile allows them to see.

Further control is provided via endpoint compliance checking. This is a feature of SSL VPNs that manage a remote user's application access based on the profile of their endpoint device when compared to a corporate security policy.

With this powerful feature it is possible to allow access only to users whose laptop meets stringent security policies. For example, in order to get access to a full range of resources, an organisation can set a policy that demands that a laptop must have a corporate firewall, anti-virus and spam blocker installed. At login time, the laptop will be scanned to determine the level of security installed on it and the SSL VPN will use this information to make decisions as to the level of access that is then provided to the remote worker. If the endpoint meets part or none of the corporate security policies it is possible to restrict access to a range of 'read only' applications and to block all downloads or uploads between the device and the network.

Data Integrity

Providing remote access to a broad range of remote users is an excellent way to increase productivity and stakeholder relations. But providing access to central resources and applications is only part of the story. One also has to consider data integrity.

SSL VPN technology should also include functionality to protect against data leakage. A good example of this would be session integrity and attachment wiping. These are features that manage data at the endpoint and ensure that corporate or confidential data removed from the device after a

session ends. It is typical for an SSL VPN to overwrite the hard drive, clear down the browser cache and delete any forms and password history when a remote session is terminated. This prevents other users from accessing data that relates to an earlier session, thus providing a strong control mechanism against data leakage.

Application Manipulation

Data leakage can be further mitigated by the use in some high powered SSL VPNs of application manipulation. In some solutions it is possible to configure the SSL VPN to act on behalf of applications and present only specific data depending on the level of trust of the endpoint device. For example, to enforce strict read only access of email, it is possible for the SSL VPN to act on behalf of Exchange and 'grey out' any action buttons such as "Forward", "Reply" and "Send". In confidential reports it is also possible to blank out sensitive data such as account numbers when a form is being viewed from an unmanaged device.

Such powerful access control is an excellent foundation stone for delivering a first class user experience. However, deploying an SSL VPN alone will not comply fully with the Code of Connection. In order to do that, a two-factor authentication solution must be added to ensure that only authorised users obtain access to restricted resources.

User Experience

SSL VPN delivers an easy to use solution because of the nature of the browser-based interface.

But the user experience does not end there. Most SSL VPNs provide support for Single Sign-On (SSO) which will allow users to login to applications automatically and without having to remember passwords. In addition, an SSL VPN pulls all applications into a single location which means that the user can access everything they need from a single portal.

The combination of a browser-based interface and a centralised application portal makes an SSL VPN a strong option when compared to other application access solutions such as IPSEC VPN.

Two-factor Authentication with One-Time Passwords

The introduction of a two-factor authentication (2FA) solution is in itself a serious consideration that needs to be reviewed carefully. There are a number of providers and form factors to consider before making a choice. With most of the higher quality SSL VPN solutions however, it is possible to integrate with existing solutions. So if you have a Public Key Infrastructure, or existing 2FA solution, you may well be able to re-use this for CoCo compliance.

Using a one-time password is common practice in two-factor authentication solutions. As the name suggests, a one-time password, or OTP, is a password that can be used for only one authentication process in order to gain access to a system. By using one-time passwords, the probability of an attack

relying on the interception and replay of network traffic is lessened because a previously valid password will not be accepted on a second or following round. OTP's are generated using various technologies, algorithms and timing sequences and are delivered to the user via various methods. Here we look at those methods in more detail.

Hard Tokens

Most traditional two-factor authentication solutions include the use of a hard token. This is a dedicated device that is used to generate a one-time password. Such solutions are both effective and prolific in the market today and the technology is readily understood. However, hard tokens come with one major weakness. Cost! Because hard tokens are physical, there is always an upfront cost to procure them. And this cost can be relatively high when compared to alternative solutions. Furthermore, tokens have a finite battery life, at which point they will cease to work and must be replaced.

But cost is not just restricted to the procurement of tokens. When deploying the solution an organisation must find a way to issue the hard token to each remote user. The user base for such tokens is nearly always made up of remote workers and so provisioning of tokens often means either sending the tokens out to all users via a secure or recorded delivery mechanism, or asking all remote users to travel to a corporate office to pick up their token. In either case, the indirect costs related to deployment of two-factor authentication can be high.

One alternative to traditional hard tokens is a smart card solution. Smart cards can provide an OTP in much the same way as a hard token, but in addition they can also provide extra services such as building access, certificate storage and single sign-on. As a result, smart card solutions can deliver significant extra value and make the 'one card' utopia a real possibility.

However, smart card provisioning for logical and physical access can be labour intensive and costly and may not be necessary in many environments.

Soft Tokens

An alternative to hard tokens is the soft token. This is a software application that can be deployed on a laptop or mobile device. Soft tokens can generate an OTP from a user interface on the mobile device and this OTP can then be used along with a PIN number to obtain access via a VPN.

Soft tokens are an interesting option for many organisations because they can help to reduce the cost of authentication whilst also leveraging the existing investment in mobile devices. Cost reductions come in two ways:

- First of all, the token itself is software and not hardware, so the associated up-front cost can be significantly lower.
- Second, the provisioning process can be quick and easy with many providers offering a provisioning website or making the soft token available through windows mobile updates or the iPhone app store.

Clientless Authentication

Another solution, referred to as clientless authentication, requires even less cost. This solution leverages the mobile phone SMS network for delivery of an OTP to a remote user through their phone handset.

Solutions like this provide a low initial cost of ownership and the deployment time is also negligible. A user repository only needs to hold user login details and the mobile phone number. Provisioning and management of the user's access is also easy. When a user leaves the organisation their access can be terminated simply by deleting their mobile phone number.

One real benefit of this solution is the user experience, which requires no real IT experience and only a simple knowledge of how to receive an SMS message. A remote user simply has to request that an OTP be sent to their mobile phone and once it arrives it can be used along with a PIN number to obtain access. Do bear in mind SMS costs though and the tariffs your organisation has signed up to.

Conclusion

When meeting the Code of Connection the type of two-factor authentication and SSL VPN platform is open to choice and it is up to each organisation to assess the market and available options.

Oxford Computer Group (OCG) can help make sense of the many options available and how to integrate these with a wider strategy for identity and access management. OCG deliver fully integrated solutions for secure remote access and two-factor authentication. See solution overviews, online demonstrations and details of our three-day Proof of Concept at www.oxfordcomputergroup.com/CoCo.