



Creating an Accreditable Remote Working Solution

A ten step guide for Local Authorities

Becrypt Guide
October 2009

Introduction

Mobile and remote working is moving up every organisation's agenda. In part, it's in response to the government's Flexible Working Regulations published in 2002. It's also a reflection of the increasing realisation that remote working represents an opportunity to offer staff a better work/life balance and so improve overall productivity.

With the legislation opening up the opportunities for flexible and home working, organisations in both the public and private sector are faced with new challenges. They are required by law to protect personal data, while allowing access to corporate systems.

Central Government has long had a culture of data protection, and in more recent years the practice of Information Assurance (managing information-related risks)¹ has since started to be applied both in local government and corporate organisations.

Why do you need an Accredited Remote Working Solution?

With remote working the boundaries change. For IT departments in local government the challenge is to maintain network security and data integrity, while enabling multiple methods of accessing files – including email, remote access and intranet.

Home computer systems and portable computers connecting from remote locations to the Internet or other networks across the Internet are increasingly vulnerable to external attack. The growing threat of malicious code - such as malware and viruses - and attempts by others to illegally gain access to computers makes it more important than ever to ensure that desktop and portable computers are as secure as possible.

For local governments, solutions in place must conform to CESG (the UK Government's National Technical Authority for IA) guidelines for products, policies and procedures for Information Security.

Such organisations must also adhere to the Code of Connection, the document that defines the minimum standards and processes that an authority must comply with before being able to connect to GCSX, (Government Connect Secure Extranet), the secure private Wide-Area Network (WAN) which enables secure interactions between connected Local Authorities and organisations.

This document provides a guide on how Local Authorities can approach these issues, for ease of use it has been split into two parts:

- **Part 1** - the ten steps required to gain accreditation for your Remote Working Solution
- **Part 2** - how to comply with the CESG Good Practice Guide for Remote Home Working and how to comply with the GSi Code of Connection (CoCo) for GCSX

Part 1. The ten steps required to gain accreditation for your Remote Working Solution

Step One – Carrying out the initial research

In order for your remote working solution to achieve accreditation it will need to comply with government legislation and standards for security. From the outset it is important to ensure that there is backing for compliance at the highest board or director level. It is also important to identify funding streams that are available to finance additional IT products and infrastructure changes that may be required.

At the same time, detailed research is required to identify the data owners within your organisation, as well as the data users and access required.

Step Two – Preparing your project plan

It is important to prepare a clear project plan. Many projects are unsuccessful because the requirements, objectives and deliverables are not clearly stated at the outset. The plan should outline timescales (start and end date) and resources required, including the staff and skills required to implement the project.

The team of personnel should be picked to match the skills required and be able to provide the time to work on the project. Clear milestones and checkpoints should also be built in, to track the progress of the project. This will highlight if there are factors that might cause delays and what needs to be done to adjust the plan.

Cost implications on the solutions available must be detailed from the beginning – it is worth obtaining advice on the options, rather than just selecting one choice. If you are uncertain, then you should ask a CESG Listed Advisor Scheme (CLAS) consultant.

Step Three – Determining the data protection levels

Early in the project you should identify at what level the data needs to be protected. It is important to review all data that is in the public domain, and then to the next level of data protection, impact levels IL 1 and 2 (which may contain personal data, names and addresses, date of birth).

If the data to be accessed contains more details, such as bank information, then the level required may be IL3.

Step Four – The Technical Architecture

Prepare your technical architecture and framework with clear diagrams. It is much easier for a compliance officer to review the proposed network and data access on a diagram and identify quickly any areas of vulnerability.

A good technical architecture will clearly illustrate how the data will flow from one point to the next, whether it passes through the Internet or via a Virtual Private Network or a Citrix gateway.

The flow diagram will need to conform to Her Majesty's Government (HMG) and International standards (ISO27001) and those outlined in the CESG Good Practice Guide details the security information standards for encryption and remote working.

Step Five – Setting up your proof of concept

The proof of concept is an important stage in your project to test the solution and see the results. A run of at least four or five weeks is recommended, with a test at the end of the period. If the system is high level security, then penetration testing is recommended. This should then be followed with an IT health check (a vulnerability type Penetration test, that needs to be carried out by a suitable qualified practitioner). Such testing should be an ongoing process, not just part of the initial pilot.

Step Six – Documenting your project

Documenting your project, including physical, procedural elements, personnel and technical information is an important part of the compliance. The document should detail from day one the initial scoping and specification, through to delivery, implementation and operational phases before going live.

Version changes should be noted, since the document will be dynamic, noting any system and other changes as and when they occur. The technical solution is the easy part of the project, the physical, procedural and personnel aspects of the remote working solution are the challenging aspects to ensure that it meets the needs of the compliance and accreditation process.

Due diligence must be given to who physically will have access to the data and whether vetting procedures have been put into place. Security controls must be in place for data handling and backup and storage processes, as well as user guides and training for the remote security tools that are in use.

Step Seven – Seeking guidance

Always seek guidance if you are unsure about any aspects of compliance. It is important to have the compliance documentation quality checked before submission. An independent body can check the documents to ensure that nothing is missed and that the whole project meets the required standards. It is worth covering this aspect early on, since last minute checks and changes may incur more cost.

Step Eight – Include a regular maintenance plan

A system should be monitored from cradle to grave. Regular maintenance should be built into your plan after your system goes live, with anti malware and patches. Antivirus and anti malware patches need also to be regularly updated, (ideally these should be automated) and audits should ensure that the system is running well.

You should also consider a disposal policy – how will you dispose of old data and obsolete or out of date hardware? Any CDs or memory sticks that have been used need to be disposed of mindfully and following clear procedures.

Step Nine – Include a disaster recovery plan

While the system is up and running, it is easy to forget that there needs to be a backup plan in the event of a failure. A robust recovery plan to ensure that business continues to be operational needs to be put into place.

Step Ten – Apply for Accreditation

With a fully detailed, accurate project plan following all of the steps outlined, you can now apply for Accreditation for Secure Remote Working. With the authority to go live with your system, it is key that the regular maintenance schedules, procedures and policies are adhered to, to ensure robust, secure remote working.

Part 2. How to comply with the CESG Good Practice Guide for Remote Home Working and the GSI Code of Connection

Whilst Government Connect can provide help and advice, meeting the Code of Connection remains a responsibility of the Local Authority.

The GSI community has revised the Code of Connection that controls access to the GCSX circuits provided by the Government Connect. Compared with Code of Connection version 3.2, one of the main areas of change in Code of Connection 4.1 is on mobile working. “[the] change in perception of threats that has led to Code of Connection 4.1 developments towards acceptance of mobile/ home working using non-authority owned equipment”².

The GSI Code of Connection for GCSX³, (Impact level 2), Version 4.1 also details that for mobile/home working any mobile/remote and or home working solution must meet the HMG IA policy and Guidance.

It specifies that data at rest on a remote device, or in transit is encrypted, using a FIPS 140-2 with CCTM approved product. The document also stipulates that:

- any use of portable electronic devices will be authorised, managed and configured and operated in accordance with CESG guidance.
- all remote connections must be from authorised official and/or managed services and records of activity are maintained (e.g. on Home PCs).
- personal firewalls must be installed and enabled and two factor authentication must be used for remote access from remote working devices.

The recent CESG Good Practice Guide clarifies the issue of bootable media usage in the organisations that handle IL 3 data. The document is available for download from the CESG GSi website, and Local Authorities may also request the document from the Government Connect. The key points for mobile/home working using non-authority owned equipment are: bootable media can be used for handling IL3 data; and the use of personal equipment is strongly discouraged “without bootable media”. However, we do recommend that you read the full document to form your own view.

Enabling secure home working

A bootable media solution offers Local Authorities an option to enable home working, without the need to supply machines to staff. Typically a USB stick, it boots into an environment that is isolated from the host PC. From within this environment it is then possible to allow a number of business functions. The precise functions available depend on the policy of the organisation for which the bootable media is configured.

Becrypt's Trusted Client is a secure, bootable media solution that meets all of the criteria stipulated in the compliance guidelines to enable home working. It creates a trusted environment separate from the untrusted software in the home PC, from where the department can allow users to conduct some form of business.

It also provides encryption of data at rest on the media to protect that data should the media be lost or stolen. The use of two factor user authentication (password and token) is recommended to provide extra security.

It is important to note that bootable media solutions create the environment only. The solutions that are then placed within that environment, such as a VPN solution, are defined by the organisation and should be risk assessed and managed in their own right.

While Trusted Client goes a considerable way to providing secure access it needs to be implemented with other security technologies to provide a complete solution. It can support a variety of Virtual Private Networks (VPNs) including Juniper and AEP, as well as Network Access Control (NAC) components. It also has management technology to support deployment and revocation events, meeting the CESG guidelines.

Ensuring confidentiality of data

It is recommended that each home worker agrees to security operating procedures, which clearly stipulate the usage. In addition, training is suggested that advises that bootable media is stored separately from the home PC, authentication token or smart card. The home user should also undertake measures to protect the PC with a personal firewall and anti virus and anti malware software. These guidelines should all be documented in the Systems Operating Instructions.

As a further measure of security, the remote servers accessed by the bootable media session should be segregated from the main corporate network/VPN and a protective monitoring solution should be put into place.

It is important that the user follows the correct boot order for bootable media solution (booting media before the hard disk) to ensure the PC does not masquerade as the bootable media. Trusted Client provides the correct boot order to meet compliance in this potentially vulnerable area.

Adopting a bootable media solution and following the ten steps as outlined, a Local Authority can be assured that its solution for remote working is robust, secure and meets all of the CESG Information Assurance requirements to be fully accredited.

A more detailed version of this guide, highlighting the numerous documents and the technical architecture you need to set in place for an accreditable remote working solution, is available upon request. Please email us at info@becrypt.com or call us on 08458382050.

¹ Becrypt Guide to Information Assurance, October 2009; Becrypt Information Assurance Risk Management Document (October 2009)

² Government Connect Newsletter Issue 11 - www.govconnect.gov.uk

³ The GSI Code of Connection for GCSX (Impact level 2), Version 4.1

#becrypt

All product names referenced within this document are trademarks or registered trademarks of their respective companies.

Becrypt Ltd disclaims interest in the marks or names of others. While every effort has been made to ensure technical accuracy, information within this document is subject to change without notice and does not represent a commitment on the part of Becrypt Ltd.

No part of this document may be reproduced or transmitted in any form, electronic or otherwise, without the expressed consent verbal or written of Becrypt Ltd.

Becrypt Ltd
90 Long Acre
Covent Garden
London WC2E 9RA
United Kingdom
t: 0845 838 2050
f: 0845 838 2060
info@becrypt.com
www.becrypt.com