End User Computing in U.K. Government: A Microsoft Approach

Abstract

This paper describes the Microsoft view of how best to deliver modern, usable, high-performing end user computing within the U.K. Government today. It explains how organisations can comply with the U.K. Government End User Device Strategy through a combination of the Microsoft Flexible Workstyle approach and current Microsoft technologies.

Authors

Richard Shipton (ricship@microsoft.com), Government Technology Strategist
Adam Shepherd (adamshep@microsoft.com), Infrastructure Solution Architect

Published: 15th March 2012

Microsoft

Contents

Executive Summary

Government desktop devices today are often perceived as being slow, expensive, and providing a poor user experience. They are functional at best, and offer few of the productivity and collaboration services that users regularly experience on their personal devices. Users increasingly have access to better performing IT away from the workplace, and in comparison to this they increasingly have a negative perception of their workplace devices.

Most government desktop devices still run Windows XP and Microsoft Office 2003—both of which are more than 10 years old. Furthermore, the tools and approaches used to design, deploy, and manage them are often outdated. Devices include a plethora of third-party management and security products, in addition to business applications. Their complexity and design make upgrades expensive, time-consuming, and adversely affects the end user experience.

For some time, this has not needed to be the case, but government IT has failed to keep pace with advances in technology. The U.K. Coalition Government End User Device Strategy recognises this, and provides a direction that offers the prospect of better IT experiences for users, and cheaper, better performing IT, by addressing some of the underlying challenges.

At the same time, as a response to the global trend of Consumerisation of IT (CoIT) in the Enterprise, Microsoft has launched its Flexible Workstyle strategy. This describes how users can access services, information, and people through devices that match their work styles, with a personalised experience fitting their preferences.

Microsoft Flexible Workstyle is a direct enabler of the U.K. Government End User Device Strategy. Both emphasise the importance of defining personas, workloads, and requirements, before considering IT. They both promote abstracting the device, operating system, management tools, user information, and applications.

Furthermore, they can both be realised using current Microsoft software: software that has evolved since Windows XP to meet most, if not all, of the government's management and security requirements. In many cases, the government has already licensed this software, but has seldom used it to its full extent.

By using this approach, government ICT can become more agile and better able to respond to the needs of businesses and end users. Not only can devices have a lower Total Cost of Ownership (TCO), but they can also fulfil users' needs more effectively. Public sector workers can see their information and communications technology (ICT) experience transformed, letting them collaborate more efficiently, and significantly increasing both their productivity and satisfactions levels.

This paper describes how the Flexible Workstyle approach and Microsoft software aid the implementation of the U.K. Government End User Device Strategy, and rapid realisation of the associated benefits.

Introduction

With end user expectations of IT being increasingly driven by their experience of their personal devices, Microsoft has developed an approach called Flexible Workstyle. This uses an intelligent infrastructure to provide a personalised experience to any device, through any connection.

The paper has been written to:

- Show how Microsoft Flexible Workstyle helps realise the U.K. Government End User Device Strategy
- Provide an understanding of a modern Microsoft end user experience and the Microsoft products and technologies that deliver it
- Describe how this translates to a U.K. Government workplace environment

The solutions presented here have been developed in the context of the U.K. Government ICT and End User Device Strategies, and the Strategic Implementation Plan[1]. They provide a baseline, which can be used by both government departments and outsourced suppliers to government.

Scope

For the purpose of this paper, the end user computing environment is considered to comprise:

- One or more devices — for example, PC, laptop, tablet, slate, or smartphone
- The operating system with which the end user interacts, and associated security
- Any infrastructure services required for user administration, security, and management
- The collaboration services that end users require to be productive

The intended audience of this paper is U.K. Government departments and agencies, but the information contained within can be easily adapted to meet other U.K. public sector bodies' requirements.

The paper addresses requirements for managing protectively marked information up to RESTRICTED level, as defined in the HMG Security Policy Framework[2]. The contents should be treated as a baseline for review and adaptation in line with organisational policies and attitude to risk.

This paper makes reference to current versions of Microsoft software, meaning those versions released as of the first half of 2012. A full list of this software can be found in Appendix A.

[1] http://www.cabinetoffice.gov.uk/content/government-ict-strategy
[2] http://www.cabinetoffice.gov.uk/resource-library/security-policy-framework

The Changing World of Government IT

Government IT Today

Around 650,000 desktops and laptops within the U.K. Government currently run Windows operating systems. These machines are used by both back-office and front-line workers to access information and services essential to their daily work.

The majority of IT service delivery is outsourced to private sector organisations, with applications and information hosted in dedicated data centres. Sharing of resources across government departments is not prevalent, and take-up of cloud services is in its early stages.

Most government departments operate their services, devices, and networks at RESTRICTED level or higher, using the Government Secure Intranet (GSI) or its successor the Public Services Network (PSN)[3]. There is a growing view that many users do not require this level of security and that a one-size-fits-all model is no longer cost effective.

The total cost of the hardware, software, and services that constitute a typical government desktop is significant, with the U.K. Government estimate of the annual cost of a desktop varying widely from £575 to £3,664 per user[4].

Microsoft Desktops in U.K. Government Today

Many government devices run Windows XP and Office 2003, which are now more than 10 years old. Microsoft will not provide any public support for these products after 8 April 2014, including security patches, non-security hotfixes, or incident support. Furthermore, hardware and software vendors are increasingly no longer supporting these technologies.

From a security perspective, Windows XP was designed to deal with the threats of the last century, and does not provide the flexibility or protection that the U.K. Government requires today—or in the future. Research from the Trustworthy Computing initiative shows that Windows 7 is ten times less likely to suffer from vulnerabilities than Windows XP. Reinforcing this, CESG recommends that departments use the latest browser and Operating Systems[5].

In addition to line of business applications, current government devices use products from multiple vendors to provide further security and management capabilities. This can:

- Significantly increase the cost of software licences, support, and integration
- Degrade performance and overall end user experience
- Inhibit reuse of architectures and services across government departments and suppliers

[3] http://www.cabinetoffice.gov.uk/resource-library/public-services-network
[4] Figures taken from 2011 Departmental Business Plans as published by U.K. Government departments
[5] CIAN 2010/08 and 2010/09 - Guidance for Departments using a Microsoft Operating System, and Guidance for Departments using Microsoft Internet Explorer

The majority of U.K. Government departments use Microsoft Enterprise Agreements as the most cost-effective way of licensing Microsoft software. Through these agreements, most departments have access to the latest versions of Windows, Microsoft Office and Microsoft management, security, business, and productivity software suites, but the majority have not deployed them fully. By failing to take advantage of functionality contained in more current software, the full benefits of this investment are seldom realised.

Changes Informing Future End User Device Direction

Today, technologies are increasingly emerging in the consumer market first and being adopted by business later. In government, growing numbers of users are asking to use iPads in the workplace alongside their work devices, and departments are beginning to use cloud-based services to collaborate with others inside and outside government.

As users' expectations of performance and usability are raised by their own personal devices, so the devices they use in the workplace increasingly fail to meet their needs. Many personal devices provide always-on connectivity, so users now expect their business devices to let them complete work tasks whether in the office or working remotely.

Cloud computing allows infrastructure, platform, and software to be consumed separately from one another as services. This reduces cost and enhances flexibility and agility, but also brings its own challenges concerning security and manageability. The adoption of cloud services will see the desktop increasingly become a platform through which users can access cloud-based services. U.K. Government's G-Cloud strategy[6] commits government to the adoption of cloud computing and delivering computing resources to users in an on-demand delivery model.

Procurement practices are evolving, recognising that future IT environments will be heterogeneous. The trend is increasingly to use the TCO of implementing and managing the device across its lifespan, rather than driving down the specification of each device to reduce cost in the short term.

In 2011, the coalition government published its ICT strategy, stating its aims to transform public services—cutting costs and complexity, and reducing reliance on big IT projects. These are to be achieved in addition to increasing interoperability, agility, and transparency.

There are also four sub-strategies covering G-Cloud, end user devices, ICT capability, and greening government. The End User Device Strategy seeks to specify a minimum set of standards to which end user devices should adhere, and a timeline for their implementation. Each of the other strategies will also affect future expectations of end user devices.

Government has also set a target of small and medium-sized enterprise (SME) involvement in 25 per cent of ICT service delivery opportunities. End user devices should enable rather than preclude SMEs, and this white paper seeks to support that position by providing a common approach that can be adopted by suppliers of all sizes.

[6] http://www.cabinetoffice.gov.uk/resource-library/uk-government-ict-strategy-resources

The Microsoft Flexible Workstyle Strategy

The culture of work is changing. Users are now more experienced in IT than ever before. They expect faster, more intuitive technology, uninterrupted services, and freedom to work anytime, anywhere, and on any device. With different generations in the workforce, people increasingly have unique needs based on their roles and preferences.

The Microsoft Flexible Workstyle approach has been designed to help provide secure, anywhere connections to information and people. This drives greater effectiveness through personalised experiences that anticipate people's needs, remember preferences, and adapt to work styles. These experiences are delivered from an intelligent infrastructure, which uses cloud computing and core Microsoft technologies.

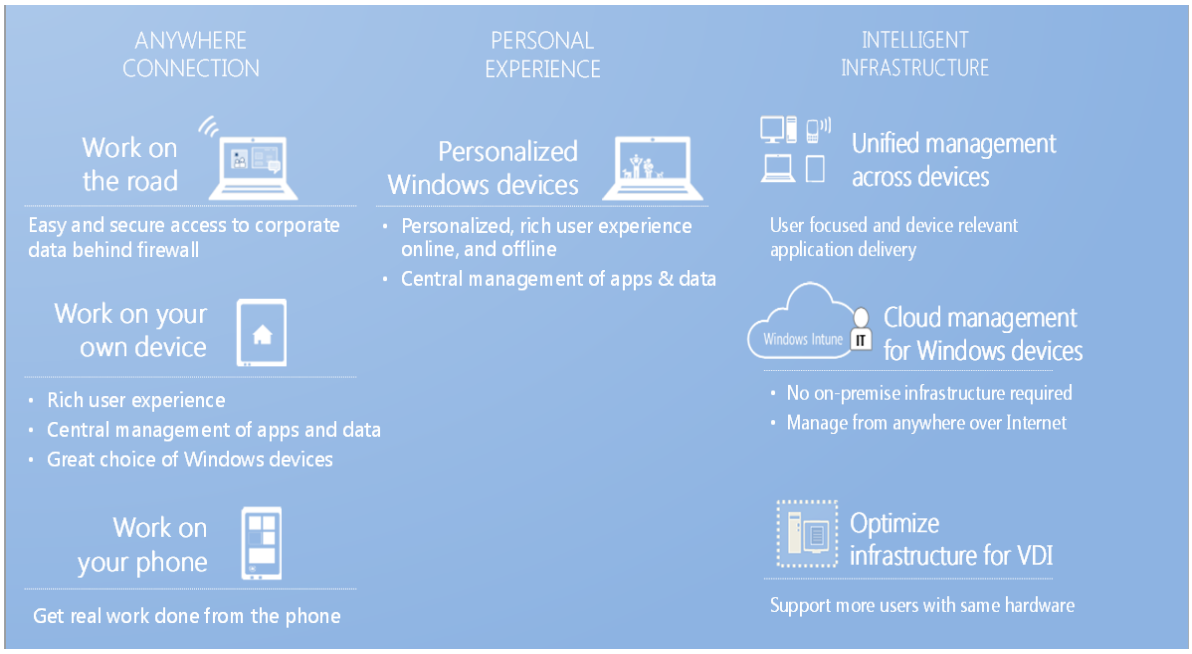

Figure 1. The capabilities that come together to deliver a Flexible Workstyle environment

To realise a Flexible Workstyle environment, Microsoft Services utilise a four stage approach:

1. Identify a set of personas that define users' characteristics, preferences, and needs
2. Develop scenarios, and determine the workloads and capabilities they involve
3. Define a distribution strategy articulating how IT services are delivered in each scenario
4. Determine the IT infrastructure requirements of the distribution strategies

Adopting a Flexible Workstyle approach offers three tangible business benefits:

- Greater productivity, because people can work where they need to, on a variety of devices and with instant access to the information they need and the people they need to collaborate with
- Improved effectiveness through tools that anticipate people's needs, remember their preferences, and adapt to their work styles
- An intelligent infrastructure that is smart, secure, cost-effective, and easy to manage

A Flexible Workstyle Approach for U.K. Government

The Flexible Workstyle approach can be adopted for the delivery of U.K. Government end user devices, but this must be done in such a way as to support some government-specific tenets:

- Align to the U.K. Government End User Device Strategy vision, goals, and standards
- Provide appropriate levels of security and compliance for the environment, and any need that the user has to access protectively marked materials
- Be easily delivered, managed, and supported by in-house government functions as well as SMEs and systems integrators
- Provide the services necessary to support and enhance end user productivity

The End User Device Strategy describes a scope for standardisation that includes devices, operating systems, application abstraction/isolation, interfaces, and device management. From Windows 7 onwards, Microsoft has promoted the same principle of separating the Hardware, OS, User State and Application. For the purpose of this paper, a simplified model is employed:

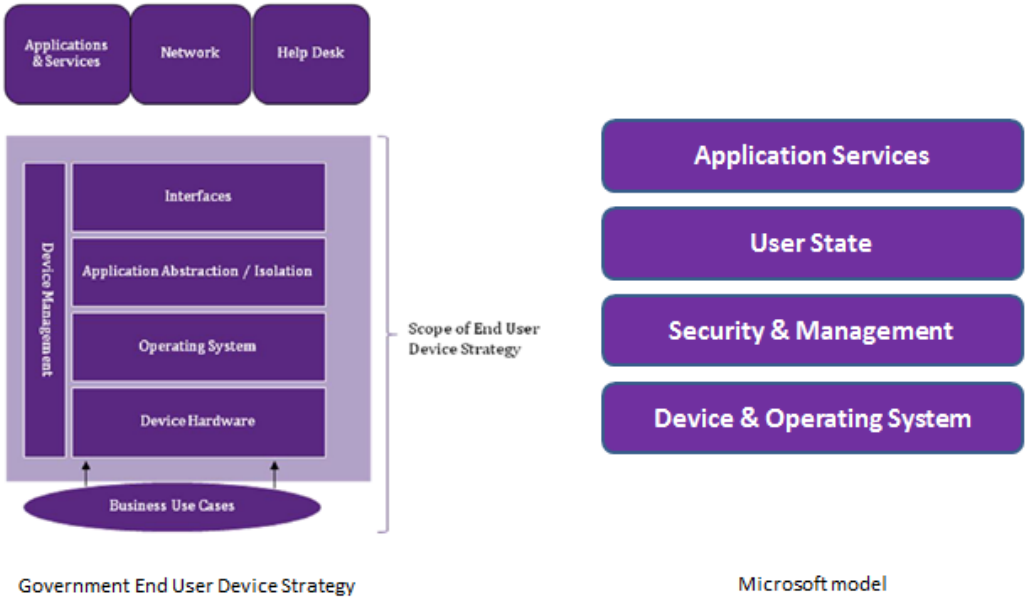

Figure 2. Government and Microsoft models for abstracting elements of the end user computing stack

The elements of this model are defined as:

- The **device** and **operating system** with which the end user interacts, which could be a PC, laptop, tablet, slate, or smartphone. The operating system can be resident either on the device or accessed remotely using some form of desktop virtualisation. Either way, it plays an important role in defining application compatibility, security, and user experience
- A **security and management** layer, which protects the device and the information on it, enforces security and other policies, collects inventory, and manages patches and updates

- The **user state**, which contains the user's settings, personalisation and (optionally) his or her personal data and files. This can be stored locally, remotely (in a data centre or the cloud) or a combination of both
- An **application services** layer through which the user accesses services, information, and line of business applications. This includes an application virtualisation technology and a browser

In addition, users require, as a minimum, access to one or more collaboration and productivity services. These could include email, personal calendars, instant messaging, document authoring, and personal and team workspaces.

The technologies required will depend on the security level at which the organisation operates, and any requirement for handling protectively marked materials. Today the majority of government departments operate at RESTRICTED level, with executive agencies and non-departmental public bodies operating at a mixture of PROTECT and RESTRICTED levels.

The following sections describe how Microsoft technology provides a baseline at each security level, which can form the starting point for a Flexible Workstyle environment for government.

Unmanaged Environment

In government, the need to accommodate unmanaged devices comes increasingly from individuals seeking to use personal devices such as iPads in the workplace, normally in addition to their official work-issued devices. Such devices are unsuitable for holding protectively marked material and controls are required to prevent users from accessing such content. Unmanaged devices can potentially introduce threats into the environment if appropriate safeguards are not in place.

Unmanaged devices would normally be permitted to join only an open network such as a department's ADSL connection, and would have no direct access to business applications or data. Such devices could, however, access line of business applications through secured remote access gateways such as Microsoft Unified Access Gateway and Remote Desktop Services.

An unmanaged device could not be connected directly to a RESTRICTED network, but with appropriate measures to protect servers and information, it is feasible to allow them to connect to a managed network in a PROTECT environment. More information can be found in the section Accommodating Multiple Levels of Security.

Where users choose or require non-Microsoft devices, they can still continue to consume Microsoft services. For example, Microsoft Office Professional Plus is available for the Apple Mac, iPad users can stay productive using OneNote, and Lync is available across a number of desktop and mobile platforms. Meanwhile, Microsoft System Center 2012 can manage a broad range of non-Microsoft devices.

There are no specific requirements for unmanaged devices, but to allow users to have access to collaboration services, Microsoft proposes the following solution:

DEVICE & OPERATING SYSTEM	• Microsoft recommends modern Windows consumer-oriented devices such as PCs, laptops, tablets, slates, or smartphones • Where users choose non-Microsoft devices, they can still utilise many current Microsoft applications and services • Users must be assumed to be administrators of their devices
SECURITY & MANAGEMENT	• Microsoft recommends Windows Intune to allow remote administration of devices, including application distribution, patching, and maintenance from the public cloud • Windows Intune to protect against malware and other threats • Alternatively, Microsoft Security Essentials, a free consumer product provides a foundation level of endpoint protection
USER STATE	• Due to the unmanaged nature of these devices, user profiles and user data would be stored locally on the device • Some user information may be stored in public cloud services • Windows Live Mesh can be used to synchronise locally held user data and settings to a Windows Live account in the public cloud
APPLICATION SERVICES	• Users working from these devices would typically not have access to the corporate network, but would use public cloud services to access email, instant messaging, and collaboration services • Applications and software is installed locally on the device or accessed via a browser • Windows Live and Office 365 contain Office Web Apps—browser-based versions of Word, Excel, PowerPoint and OneNote • Microsoft Office 2010 can be installed locally to provide rich business productivity tools

Microsoft recommends its cloud productivity services, such as the free consumer service Windows Live or paid-for subscription service Microsoft Office 365. Both provide email, calendar, instant messaging, and personal workspace functionality. Office 365 augments this with team workspaces, web sites, online meetings, audio/video conferencing, and enhanced functionality.

PROTECT Environment

This environment helps users to work with protectively marked information up to and including PROTECT level, and security measures are present to ensure access to information is controlled accordingly. Security and management is in line with recognised commercial best practice.

The physical network will be managed with perimeter controls to ensure appropriate access to resources. In addition, network security such as encryption and authentication may be employed to further restrict access to servers and information from unauthorised devices and users.

Devices can be modern, but must meet a set of criteria that allows domain management and security to be implemented in line with commercial best practice. They will often provide some form of Virtual Private Network (VPN) client to allow secured remote access to business networks.

In an environment operating at PROTECT level, Microsoft proposes the following solution:

DEVICE & OPERATING SYSTEM	• Modern Windows PCs, laptops, tablets, slates, or smartphones, deployed and supported as a managed desktop service • Microsoft recommends use of a Trusted Platform Module (TPM) • The operating system may be hosted remotely and accessed using desktop virtualisation technologies such as Virtual Desktop Infrastructure (VDI) or Remote Desktop Services (RDS) • Users' local administrator rights are removed and users operate in a standard user desktop environment • BIOS must be centrally managed and password-protected
SECURITY & MANAGEMENT	• BitLocker Drive Encryption provides encryption of fixed drives, while BitLocker to Go offers removable media encryption • Active Directory Domain Services and Group Policy provide user account, operating system, and configuration management • Active Directory Rights Management is recommended to protect emails and documents within and beyond the organisation • Windows AppLocker prevents execution of unauthorised code • DirectAccess offers seamless access to the corporate network without third-party virtual private network (VPN) solutions • System Center 2012 provides inventory, software update, configuration management, application delivery, and self-service • System Center 2012 Endpoint Protection provides antivirus and anti-malware protection and with Windows Firewall, delivers intrusion prevention
USER STATE	• Windows roaming user profiles and folder redirection store users' profiles and data on Windows servers, abstracting them from the device. This allows users to access their files and settings from any device within the environment
APPLICATION SERVICES	• Devices have access to line of business applications as well as public and private cloud services • Microsoft Office 2010 is installed locally on the device, providing rich business productivity tools • Line of business applications are isolated using application virtualisation, and can be delivered on-demand using application streaming capabilities • Users have access to a personalised portfolio of applications, which can be mandated or requested through the System Center 2012 application catalogue

Microsoft recommends Office 365 as its hosted and managed public cloud collaboration service, and Office Professional Plus. Microsoft Exchange Server, Microsoft Lync Server, and Microsoft SharePoint technologies can also be deployed on-premises as private cloud services. These can be combined as a hybrid cloud, where some users are hosted on-premises and some online.

RESTRICTED Environment

This environment helps users to work with protectively marked information up to and including RESTRICTED level, and is the standard working environment of many U.K. Government departments today.

Devices can be modern Windows devices, but operate under more specific CESG guidance for levels of security compliance, while still being managed using commercial best practice within the guidelines of departmental and government policy.

DEVICE & OPERATING SYSTEM	As for the PROTECT environment, with the following additions: • Microsoft recommends use of a CESG-assessed TPM • Users' local administrator rights are removed and functionality is further controlled using the Government Assurance Pack (GAP)
SECURITY & MANAGEMENT	As for the PROTECT environment, with the following additions: • The GAP should be applied to provide a RESTRICTED level of compliance and auditing through Group Policy and AppLocker • BitLocker Drive Encryption delivers encryption of fixed drives while BitLocker to Go provides removable media encryption, configured in line with CESG guidance • Additional auditing may be required, enabled via Group Policy
USER STATE	As for the PROTECT environment
APPLICATION SERVICES	As for the PROTECT environment, with the following additions: • Use of public cloud services should be in line with customer requirements for information security

Microsoft recommends a collaboration environment based on Exchange Server, Lync Server, and SharePoint technology. To enable collaboration on materials classified up to RESTRICTED level, software would need to be either deployed on-premises or consumed from an appropriately accredited service provider.

Accommodating Multiple Levels of Security

Flexible Workstyle includes the concept of users working on their own devices. Today, however, government has specific security requirements which largely prohibit users from accessing applications and protectively marked information on their personal devices. This section describes approaches through which different security levels can begin to co-exist, and how IT environments can start to become more heterogeneous.

Unmanaged devices cannot currently be introduced onto a RESTRICTED network because of the security requirements of the GSI Code of Connection. Meanwhile, many government departments operate at RESTRICTED level by default, while also acknowledging that the majority of users rarely handle such protectively marked information.

It is possible to create an IT environment where both managed and unmanaged devices can be accommodated, using currently-available technologies. With the right combination of organisational policy, security controls and technology to manage access to specific resources, it is feasible to:

- Operate a managed departmental network at PROTECT level, whilst RESTRICTED information is protected by server hardening and transport layer network encryption
- Allow unmanaged devices to access a managed network (at PROTECT level), and specific information and/or services which have been hardened against unauthorised access

- Allow internet-connected devices to “browse up” to more secure environments, and access specific protectively-marked information in a tightly-controlled manner (referred to as a “Walled Garden” approach)

Microsoft provides a number of technologies which support their implementation:

- Network encryption and authentication technologies such as IP Security (IPsec) can be used to restrict access to internal servers through domain and server isolation architectures. This can contribute to allowing a degree of network sharing across security levels.
- Active Directory Rights Management Services provide a mechanism for restricting access to protectively marked materials. If combined with IPsec[7], it can prevent users working on unmanaged devices from accessing materials even if the users themselves are authorised.
- Remote Desktop Services (RDS) and Virtual Desktop Infrastructure (VDI) provide a means for remote access to user desktop Operating Systems, applications and settings. This can be combined with managed security gateways, such as Forefront Unified Access Gateway, to help prevent unauthorised access to protectively marked and sensitive information.

These capabilities address a number of the Flexible Workstyle scenarios discussed earlier in this paper, but must be utilised in line with organisational security requirements and attitude to risk.

[7] As of January 2012 IPsec has not yet been evaluated by CESG. It should be deployed in line with organisational risk management policy, and its use discussed first with departmental accreditors. Microsoft expects that, as part of any formal evaluation of Direct Access, the IPsec components of the Windows 7 networking stack would need formal evaluation

Benefits of a Flexible Workstyle Environment

Reduced Costs and Complexity

The Flexible Workstyle architecture is optimised and extensible, allowing organisations to minimise initial costs by "starting small", but without incurring cost from rework and duplicated infrastructure when new workstyles are added.

Software license and integration costs are minimised by fully utilising Microsoft software which the customer already has rights to, and taking advantage of native Windows functionality, e.g. Hyper-V.

Application virtualisation reduces software development, integration and management costs, whilst eliminating dependencies between the application and device makes reusing and sharing easier.

Cost and complexity is further reduced by ending a one size fits all approach to security and devices.

More Agile, Responsive End User Computing

The Flexible Workstyle architecture allows devices and services to be added and changed more quickly and cheaply, by minimising the need for infrastructure design, integration and testing.

Virtualisation, coupled with a self-service application catalogue, allows line of business applications to be provisioned and de-provisioned more quickly.

Expensive, disruptive and infrequent upgrades can be replaced with continuous improvement.

Improved End User Experience and Greater Productivity

The Flexible Workstyle approach ensures users have a device and experience personalised for their role, and that they have access to the services and information they need, when they need them.

Unproductive time is reduced through faster application loading, start-up and shutdown times measured in seconds not minutes, and a familiar end user experience more akin to a personal device than a traditional government desktop.

By providing integrated access to collaboration tools such as instant messaging and online meetings, users are able to engage colleagues and share information more quickly and effectively.

End User Computing Which Is Aligned To Government Strategy

Green benefits are realised through reduced infrastructure requirements, greater use of cloud services, and reduced device numbers. Current versions of Windows contain numerous features and improvements to reduce power consumption, increasingly so when coupled with modern devices.

Flexible Workstyle utilises current Microsoft technology to simplify the de-coupling of the device, operating system, user state and applications. This not only meets the requirements of the End User Device Strategy but also increases flexibility and mobility, helping meet government goals for estates rationalisation and anywhere working.

Appendix A: Microsoft Technologies Used

Operating System and Browser

Technology	Summary Description	Relevant Capabilities
Windows 7 Enterprise	Windows 7 is the most advanced Microsoft Windows operating system for the enterprise. Windows 7 helps achieve lower total cost of ownership for the desktop by enhancing productivity, increasing security, and streamlining management A Windows 7 desktop operating system can be locally-installed, or delivered using desktop virtualisation e.g. VDI or RDS	End user operating system
Internet Explorer 9	Internet Explorer 9 is the latest Microsoft browser, which introduces a clean look and feel, hardware acceleration, and support for modern web standards such as HTML5. For the enterprise, there are numerous security and management features, configurable using Group Policy	Access to browser-based applications

Security

Technology	Summary Description	Relevant Capabilities
Microsoft Security Essentials	Microsoft Security Essentials is a free download built for individuals and small businesses, to protect against viruses and spyware. It is based on the same technology that Microsoft uses in its enterprise products	Antivirus Anti-malware
System Center Endpoint Protection (Previously Forefront Endpoint Protection)	Microsoft System Center Endpoint Protection simplifies and improves endpoint protection while helping to reduce IT infrastructure costs significantly. It builds on System Center Configuration Manager, allowing customers to use existing client management infrastructure to deploy and manage endpoint protection. This lowers ownership costs while providing improved visibility and control over endpoint management, and proven, accurate detection of known and unknown threats	Antivirus Anti-malware
BitLocker BitLocker To Go	BitLocker and BitLocker To Go provide encryption of both fixed disks and removable media. BitLocker Drive Encryption helps protect sensitive data from being accessed by unauthorised users who come into possession of lost, stolen, or improperly decommissioned computers BitLocker to Go extends protection to USB storage devices, enabling them to be restricted with a passphrase. In addition to having control over passphrase length and complexity, IT administrators can require users to apply BitLocker to removable drives before being able to write to them	Password-protected full disk encryption Protection of removable media

DirectAccess	DirectAccess enhances the productivity of mobile workers by connecting them seamlessly and more securely to their corporate network any time they have Internet access—without the need for third-party VPN solutions	VPN-less access to departmental networks and resources.
AppLocker	AppLocker helps to restrict exactly which software can be installed and executed by end users. Folders and files can be blacklisted and whitelisted using Group Policy, based on name, vendor, version, and other attributes	Malware and virus protection Prevent circumvention of security controls
Government Assurance Pack	The Government Assurance Pack (GAP) provides a CESG approved IL3 baseline configuration for Windows Enterprise computers	IL3 compliance

Management Services

Technology	Summary Description	Relevant Capabilities
Windows Intune	Windows Intune simplifies how businesses manage and secure PCs. It delivers public cloud-based management and industry-leading security capabilities from a single web-based console—so computers and users can operate at peak performance from anywhere With the simple setup of the cloud service, costly deployment and time-consuming maintenance are eliminated	Manages devices remotely Installs and manages software, patches and settings. Manages licence agreements. Helps ensure devices are secure—includes Endpoint Protection
System Center	The Microsoft System Center family of products and solutions encompasses a variety of leading IT management solutions. System Center solutions capture and aggregate knowledge about the infrastructure, policies, processes, and best practices so that IT pros can optimise IT structures to reduce costs, improve application availability, and enhance service delivery	As for Windows Intune, plus: Managed data centre infrastructure and applications. Manages non-Microsoft end user devices Provides a software catalogue from which users can self-install software. Manages software approvals, licences
Active Directory Rights Management Services	Active Directory Rights Management Services (AD RMS) provides a comprehensive solution to help protect and control access to sensitive information, such as documents and email messages, both during and after their delivery Authors of information can define exactly how the recipient can use information, including who can open, modify, print, forward, and/or take other actions In addition, AD RMS offers custom-use policy templates such as “Company Confidential—Read Only” that can be applied directly to sensitive information	Prevents unauthorised access to information both within and outside government Supports enforcement of protective marking scheme When combined with network management (IPsec) prevents protectively marked information from being accessible on unclassified devices
Active Directory Domain Services	Windows Domain allows administrators to manage devices and user accounts, using technologies such as Active Directory and Group Policy. This allows control over aspects such as security and user experience, using the large number of granular controls	Enforces device security through Group Policy Centralised management of user accounts

Applications and Services

Technology	Summary Description	Relevant Capabilities
Microsoft Office 2010	Microsoft Office is our best-in-class productivity suite, providing Microsoft Outlook, Word, Excel, PowerPoint, OneNote, Publisher, Access, InfoPath, SharePoint Workspaces and Lync	Email and Calendar Content creation and collaboration
Windows Live	Windows Live is a public cloud service that enables users to communicate from anywhere, with anyone, in any way they want Windows Live allows consumers to easily access, organise, and share their digital information across devices and services Windows Live is accessible to anybody free of charge through www.live.com	Email Personal workspace Document sharing and collaboration Instant messaging Browser-based document editing
Office 365	Microsoft Office 365 brings together cloud-based versions of the Microsoft email and collaboration software with our familiar Microsoft Office Professional Plus suite Services are licensed on a per-user per-month basis, so users need only be provisioned with the services they require for their roles It provides anywhere-access to email, documents, contacts, and calendars on nearly any device, and works seamlessly with Microsoft Office and the other programs users already count on every day Office 365 can also be combined with traditional on-premises deployments of email, SharePoint, and Lync, where certain users or groups require additional capabilities or levels of security	Email (Microsoft Exchange) Personal and team workspaces (Microsoft SharePoint) Instant messaging, audio and video; online meetings (Microsoft Lync) Browser-based versions of Microsoft Word, Excel and PowerPoint, and full versions of Office Professional Plus Support for a broad range of both Microsoft and non-Microsoft devices, browsers, and operating systems