



DEFENCE INDUSTRIES
Council



Defence e-Business

A Guide to Commercial Issues



Endorsed by:

Office of the e-Envoy
Leading the drive to get the UK online



OGC
Office of Government Commerce

MOD/INDUSTRY COMMERCIAL POLICY GROUP

GUIDELINE NUMBER 6

Editor	Symon Lydiard
Deputy Editor	Grant Lovett
Published by	Business Information Publications Ltd Park House 300 Glasgow Road Shawfield Glasgow G73 1SQ
Tel:	0141 332 8247
Fax:	0141 332 2652/2792
Email:	bip@bipcontracts.com
Website:	www.bipcontracts.com

Other guides in the MOD/Industry Commercial Policy Group series can be viewed at:
<http://www.ams.mod.uk/ams/content/docs/toolkit/ams/admin/navigation/frames.htm>

CONTENTS

	–	Foreword	4
Chapter 1	–	Introduction	5
Chapter 2	–	The Law	9
Chapter 3	–	Document Management	11
Chapter 4	–	Public Key Infrastructure and Electronic Signatures	16
Chapter 5	–	Defence Electronic Commerce Service	23
Chapter 6	–	e-Purchasing	26
Chapter 7	–	Collaborative Working	29
Chapter 8	–	e-Tendering	34
Chapter 9	–	Reverse Auctions	38
Chapter 10	–	Government Procurement Card	41
Chapter 11	–	The e-Business Revolution	44
Annex A	–	List of MOD Conditions and Related Guidance	48
Annex B	–	List of Contact Names and Addresses	49
Annex C	–	Glossary of Terms	51

FOREWORD



Stan Porter
Director General Commercial
Ministry of Defence

by



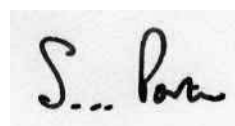
David Scillitoe
Chairman
CBI Defence Procurement Panel

In 1999, we were pleased to write the Foreword to *A Guide to Contracting for Information in the Electronic Environment*. That publication sparked a good deal of interest in e-Business by the Defence commercial community.

In the interim, the MOD and many of its trading partners have made major strides in the introduction of e-Business techniques – for example the launch of the Defence Electronic Commerce Service, the EXOSTAR exchange and the creation of many project-related Shared Working Environments.

The MOD's commercial policy has kept pace and, in some cases, has been ahead of these developments. This is due in no small part to the open and co-operative working relationship that exists between the Department and Industry. This guide is a product of that relationship, being jointly produced by a team of MOD and Industry representatives, and we are pleased to endorse it as such. It replaces the 1999 guide and also forms part of a suite of guidance produced under the aegis of the Commercial Policy Group – a joint MOD/Industry senior-level committee formed to consider the future development of commercial policy including commercial issues raised by Smart Acquisition.

We commend this guide to commercial managers, and others with an interest in the subject, working in the MOD and the wider Defence Industry community.



CHAPTER 1

INTRODUCTION

By Simon Lydiard

MOD Commercial Policy Adviser on e-Business and Guide Editor

WHAT IS E-BUSINESS?

The subjects discussed in this guide and the terminology used often prompt a good deal of confusion. In the field of e-Business, a number of terms seem to be used interchangeably or with little thought as to their meaning – e-Commerce, e-Business, e-Procurement etc.. In a fast changing environment it is not surprising that one of the fastest areas of growth is in the creation of new "buzz words". On the whole it is not necessary to worry unduly about the different terminology. However, there is one distinction which is worth making.

For the purposes of this guide, we take the phrases e-Commerce and e-Business to mean:

- e-Commerce is the electronic conduct of buying and selling activity and is usually associated with websites from which consumers purchase goods or services (known as b2c – business to consumer), but it is also used in relationships between businesses, often employing private networks (b2b – business to business). In the defence sector, the MOD in particular, we are largely concerned with this latter category of e-Commerce – although the former may have some relevance, for example when using the GPC.
- e-Business is a broad term, embracing all of the individual "e" tools and techniques. It is usually taken to mean the integration of electronic processes beyond buying and selling activities, e.g. full integration into organisations' ERP (Enterprise Resource Planning) systems or equivalent business tools to conduct transactions by electronic communications end-to-end.

In the defence environment a number of tools and techniques are available which, collectively, add up to a full range of e-Business capabilities.

Some examples are shown below:

e-Mail
e-Procurement
e-Commerce
e-Process
e-Working
Full e-Business!

BENEFITS & RISKS

e-Business must be about delivering benefits. It is not about applying electronic techniques just to be fashionable. Many of the benefits will be articulated in subsequent chapters where individual subjects are addressed. However, there are some generic benefits to be realised which fit broadly into the SMART Acquisition philosophy of "*Faster, Better, Cheaper.*"

- **Faster:** The application of e-Business techniques enables the realisation of business process redesign, using electronic tools to speed up processes, often by means of automation;
- **Better:** Working electronically enables people to be liberated from routine, non-value-adding tasks. It makes the computers do the drudgery, freeing up the power of human intellect and creativity. Working electronically also offers improvements in traceability and auditability;
- **Cheaper:** Automation and taking manual intervention out of the equation can lead to reduced costs.

There are also broader, governmental benefits to adopting e-Business techniques. The Prime Minister stated that he wished the UK to provide the best environment in the world for e-Trading¹. In that context, public sector procurement organisations can act as exemplars, using their purchasing power to encourage the adoption of e-Business techniques, and thereby assisting the development of the UK marketplace. In order to encourage government departments to engage in this process, the Government has set down the aim of undertaking all service provision electronically by 2005. Ultimately, however, decisions on the application of particular techniques have to be based upon the business value that these techniques deliver.

Working in this new environment is not without its risks. In the defence sector, in particular, the UK is working on the boundary of new developments, pushing the agenda forward. For that reason, we are encountering new issues well ahead of other areas. Individual chapters of this guide will address risks as well as benefits in respect of particular subjects. Nevertheless, there are also some generic risks. Perhaps the biggest of these is that, unlike most manual business processes, e-Business is very often supported by one or more third parties, who are not part of the usual business relationship, for example providers of exchange services like the Defence Electronic Commerce Service (DECS) and EXOSTAR. The existence of these third parties has to be recognised in business relationships and there has to be clarity about which parties are responsible for particular risks and who bears liability for them.

While there are new risks to be addressed as a result of implementing e-Business, merely from the use of electronic transactions, all the normal rules, legal principles and rules of business in a non-electronic environment continue to apply.

¹'By 2002 the UK will have the best environment in the world for electronic trading.' Rt Hon Tony Blair MP, 1998 Efficiency White Paper.

E-BUSINESS IN DEFENCE

The Ministry of Defence and those of its suppliers who are its major Industrial partners are committed to employing e-Business techniques in their trading and collaborative relationships. The Department has published an e-Business strategy² and many of the major defence industries also have strategic visions of how they are employing or intend to employ e-Business.

JOINED-UP GOVERNMENT

The MOD works closely with other government departments and agencies to ensure that its application of e-Business takes into account wider government interests. The Department's e-Business strategy is approved by the Government's e-Envoy, with whom it has a close working relationship. MOD also works closely with the e-Commerce Team at the Office of Government Commerce (OGC) and are represented on a number of the OGC's "e" committees. The OGC has the policy lead in central civil government for e-Commerce. Both the e-Envoy and the OGC are represented on a defence e-Business committee, which reports to the Commercial Policy Group³.

MOD AND INDUSTRY WORKING TOGETHER

There are a number of committees, organisations and initiatives in the e-Business arena demonstrating the desire of the MOD and its Industrial partners to work together for mutual benefit. For example, the UK Council for e-Business (UKCeB) sponsors a number of Working Groups that each look in detail at specific aspects of e-Business, such as Information Management and the Export Control of Intangibles. In the context of commercial issues, a working group has been formed under the auspices of the Commercial Policy Group. The e-Business working group is jointly chaired by representatives of the MOD and Defence Industry and is composed of stakeholders from Defence Industry, e-Business service providers as well as MOD itself and other central government organisations, such as the e-Envoy and the OGC. The purpose of the working group is to drive forward the development of commercial policy on the application of e-Business, ensuring that the commercial approach takes account of risks and liabilities and allocates these appropriately. It is also a forum for new ideas and an opportunity for Industry representatives to influence MOD thinking and keep up to date with new developments.

²*Delivering e-Defence: MOD's Response to the Information Age Government Agenda (Summer 2001 edition).*

³*The Commercial Policy Group is a joint committee, comprising senior commercial representatives of MOD and Industry. It was formed in January 2001 to address commercial issues in the SMART Acquisition agenda.*

Organisations represented on the working group are as follows:-

Defence Logistics Organisation	Confederation of British Industry	Ultra SBS
Defence Procurement Agency	Office of Government Commerce	Smiths Group
Director General Information	United Kingdom Council for e-Business	BAE SYSTEMS
Defence Estates	Society for British Aerospace	Sun Microsystems
Legal Advisor	Lockheed Martin	British Telecom
Aerosystems International	Rolls Royce	Xcel UK
TRW Systems	Mass Consultants	Thales Optronics
Chemring Countermeasures	Cap Gemini Ernst & Young	
Enterprise Integration Programme Coherence Team	General Dynamics	

Key to the commercial implementation of e-Business is the development of a portfolio of standard contract conditions that facilitate the agreement of contracts that enable MOD and Industry to take advantage of e-Business techniques.

e-Business is a challenging subject, and the more we can work from a standard tool-set of conditions, with obligations, risks and liabilities already scoped, at least at an outline level, the quicker we can get to contract. Of course, being realistic, this is an area of business where things can move very quickly, so we will never have all of the commercial issues completely worked out.

THIS GUIDE

Within the chapters of this guide, we hope to explain the various applications and techniques that are in use or could be used in commercial relationships between the MOD and its Industrial partners. Each chapter tries, in so far as is possible, to outline these in straightforward language, to explain the commercial significance, and to provide pointers to further information and contact points. Due to the dynamic nature of the subject, and the fact that the guide references other, sometimes more detailed documents, this cannot be regarded as a fully comprehensive guide to Defence e-Business. However, we believe that it does represent the first overview of the subject from a commercial perspective.

ACKNOWLEDGEMENTS

This guide could not have been produced without the following, who have contributed sections, ideas or commented upon the drafting: Jean Keay, Gwen Beale, Colin Sinkins, Denise Savage, Mary Shoobridge, Jack Danpure, Robert Miller, Jim Ayres, Julian Campbell, Anne MacFarlane, Ian Rooney, Jerry Fathers, Rick Evans, Alan Brown, Brian Duffy, Peter Farmer, Andy Carpenter, Paul Newman, Tim Lam, Simon Dunford, Graham Sturgess, Patrick Curry. I owe a particular debt to Grant Lovett, for providing valuable and extensive support in the editing process. Grateful thanks are also due to David Scillitoe, my co-Chair on the Commercial Policy e-Business Working Group, and to other members of the Working Group. Any errors or omissions are, of course, entirely the responsibility of the editor.

CHAPTER 2

THE LAW

WHAT IS THIS CHAPTER ABOUT?

This Chapter provides a general summary of some of the legal considerations associated with conducting commercial business by electronic communications. Other Chapters deal in more detail with specific legal issues.

KEY POINTS

- English law is generally permissive of e-Commerce;
- It is important that organisations conducting e-Business understand and agree on how to conduct business by electronic communications;
- EU Procurement Directives are being revised to recognise the conduct of commercial business by Public Authorities may include electronic communications.

THE DETAIL

CONTRACTING

English law requires no particular form for the creation of contractual rights and obligations. A contract can be created, providing the necessary elements are in place, orally or in writing. Accordingly, there are no legal bars to the creation of contracts by electronic communications.

PROOF

Of greater concern is establishing that a contract has been entered into and defining what the terms of the contract are. For this reason it has become established practice within the commercial world for contracts to be in writing and to be authenticated by the signatures of the parties.

WRITING

The Electronic Communications Act 2000 (the ECA), specifically Section 8, allowed Ministers to amend legislation where there existed doubt about whether that legislation would preclude use of electronic communication. The most recent Government view in relation to this aspect is that, in interpreting the word "writing" in statutes, regard should be made to what "the intent of Parliament" was, rather than a strict interpretation of the word "writing". Accordingly, it is likely that moves to amend existing legislation will be restricted to those areas where there is doubt that an interpretation of electronic communication could be applied to words such as "writing". Coupled with that view is the report from the Law Commission Electronic Commerce – Formal Requirements in Commercial Transactions dated December 2001. Although doubt remains over the status of Electronic Data Interchange (EDI) messages, there is a strong body of legal opinion which states that electronic transactions such as e-mail satisfy the requirements of the definition of writing. This is on the basis that they are capable of reproducing words in a visible form that can be read by a person (EDI is a form of electronic messaging which is read by programmed computers and does not produce "words" in the normal usage of the expression).

SIGNATURE

The ECA dealt with the issue of the admission as evidence of electronic signatures. Thereafter, the Law Commission Report on Electronic Commerce concluded that what was determinative of the validity of a signature was its function rather than any particular form. Accordingly, it concluded that digital signatures, scanned manuscript signatures, typing one's own name or initials and even clicking on a web site button could constitute methods of satisfying a signature requirement, on the basis that the "signing" party, in so doing, intended to be bound.

PRACTICE

The detail given in the earlier part of this chapter suggests that e-Commerce could operate without any constraints. It is therefore essential when conducting commercial relations, that the parties to those relations understand how they intend to contract and to be bound. What form do they intend their contracts will take? What form will be acceptable as a valid signature at specific levels in the procurement/contractual hierarchy, e.g. will it be necessary to have the same level of authentication, such as by reference to certification issued under a Public Key Infrastructure (PKI), for Quality Assurance (QA) certification as for contract signature?

JURISDICTION

In using e-Commerce, one of the major problems is determining the law that will apply to individual transactions which may be carried out by electronic communications. It is unlikely that this will have a significant impact on defence business since this should be covered by contractual provisions which set out the relevant jurisdiction. The MOD does not presently envisage that their procurements will take place over the Internet in a way that jurisdictional issues arise, as long as the contractual provisions are clear and not open to interpretation.

EU PROCUREMENT DIRECTIVES

The present Directives were put in place before the full impact of e-Commerce was known. Accordingly, they do not, in places, sit comfortably with some of the practices being developed. However, negotiations are ongoing to produce a consolidated Public Sector Procurement Directive to Facilitate e-Procurement which will deal with matters like shortened time limits for procurement based on electronic communications and Reverse Auctions.

SUMMARY

There are no major legal impediments to the conduct of e-Business, but it is important to understand how legal and procedural issues impact upon the conduct of particular activities and what can be done to reduce the risk of these issues arising.

WHO SHOULD I CONTACT TO FIND OUT MORE?

Organisations should contact their own legal departments for specific advice.

ARE THERE ANY BACKGROUND DOCUMENTS?

Electronic Communications Act 2000 www.legislation.hmso.gov.uk/acts/en/2000en07.htm

The Law Commission Report, available at: www.lawcom.gov.uk/library/lcspecial-1/e-commerce.pdf

CHAPTER 3

MANAGING ELECTRONIC DOCUMENTS AND RECORDS

WHAT IS THIS CHAPTER ABOUT?

This chapter provides guidance on how to manage electronic documents, and maintain business records, to support commercial relationships.

KEY POINTS

- Electronic documents (including e-mails) must be created, stored and managed in a systematic manner;
- The use of an Electronic Document and Record Management System (EDRMS) is recommended;
- Within the MOD unless an approved EDRMS is used, electronic documents that need to be kept as a formal record of business must be reproduced on paper and stored in a registered filing system;
- Agreements should be signed with Industrial partners covering the use of electronic documents in contractual relationships.

DETAIL

DEFINITIONS

The term "electronic document" covers any information held in electronic form. Typically these are office automation files (e.g. a Microsoft Word document) and e-mails, but they could include many other types of information, for example database reports, video and audio clips, images, discussion groups etc..

CREATING ELECTRONIC DOCUMENTS

The conduct of commercial business can generate large numbers of electronic documents. Unless these documents are created, managed and stored in a logical and consistent manner, there can be an adverse effect on business.

For example:

- Wasted time searching for files;
- Loss of control of document versions;
- Failure to re-use relevant documents and information from previous work;
- Failure to keep proper records, compromising an organisation's position in disputes or legal action because it cannot find the necessary evidence.

Organisations and project teams working across organisations using electronic communications should establish standards for creating and labelling electronic documents.

MANAGING ELECTRONIC DOCUMENTS AND RECORDS

In particular:

- The format for electronic files (e.g. Word, HTML, PDF etc);
- Use of document standards, such as templates and metadata;
- File naming conventions (including version labelling);
- Protective marking conventions;
- Format of e-mails and their attachments.

In implementing these standards it will be necessary to satisfy the requirements of the various participants and users of documents.

Many of these requirements are already well known, so there should be a consolidated effort to adhere to these requirements whilst at the same time ensuring a consistency of approach, both within your own organisation and when exchanging documents and e-mails with other organisations.

ORGANISING AND MANAGING ELECTRONIC DOCUMENTS

The majority of documents used in contractual relationships are created electronically, and in many cases communicated in electronic form via e-mail (and attachments), or by transferring files on floppy disks, CDs and other portable storage media. While the MOD, and most other organisations, have traditionally had robust procedures for managing paper documents, these have not always been translated into the electronic environment.

All organisations should therefore consider reviewing their processes for managing electronic documents to ensure they are effective, in particular:

- Electronic documents and e-mails must be kept in properly organised and managed file stores. In particular e-mails must be stored with related electronic documents (i.e. those on the same subject) and must not be left in "inboxes" or "outboxes".
- Internal organisations (MOD and Industry) should use shared file areas (where IT systems provide the necessary functionality), rather than individual file stores.
- All electronic documents and e-mails that need to be kept as formal records (as opposed to transitory working documents and correspondence) must be identified and placed in a formal record keeping system.

RECORD KEEPING

Within the MOD the current policy is that electronic records can only be kept in an "accredited" EDRMS. Therefore, if an EDRMS is not available, any electronic document or e-mail that needs to be kept as a formal record must be printed out and placed in a registered filing system. This does not rule out keeping electronic documents and e-mails for "working purposes" (for example to re-use electronic document formats, to allow other members of a group to share information, or to research what was done on previous projects or contracts).

SHARED WORKING ENVIRONMENTS

The conduct of commercial and contractual relationships often involves the generation, use and exchange of large amounts of electronic information. In these cases, consideration should be given to establishing and operating a Shared Working Environment (SWE) between the parties. This would be used to store common information, and also provide a range of collaborative working tools to help work more effectively as a team. Further guidance on SWEs can be found in Chapter 7.

WHEN TO USE PAPER DOCUMENTS

Chapter 2 provides guidance on the legal aspects of electronic documents and in general terms they can be used in the conduct of commercial and contractual relationships. However, there are risks associated with the use of electronic as compared to paper documents.

For example:

- **Reliability.** Because most e-mail systems cannot confirm delivery, important messages may get lost. Because of this uncertainty other organisations could claim that e-mails were not received;
- **Integrity.** Electronic documents can be corrupted due to system errors or amended by users, often in a way that is undetectable. This can lead to the loss of important information. This can also lead to disputes concerning the integrity of documents (for example electronic documents presented in evidence);
- **Protection.** Important documents might be lost due to system error or user action (deliberate or accidental);
- **Authenticity.** Individuals may dispute that they had signed documents. In addition, with a conventional e-mail system it is not possible for recipients to be certain that the sender of an e-mail is who they claim to be.

These weaknesses should not be overstated. Providing that electronic documents are managed properly, and excepting the potential problems detailed above, they can be used in contractual and commercial relationships. The use of digital signatures backed by robust PKI solutions (see Chapter 4), and storage of documents and records in EDRMS systems, can mitigate these risks.

In many cases the use of paper documents is driven by custom and practice rather than genuine need. Use of paper documents should be reviewed, and only continue where the risks of moving to electronic documents make the retention of paper genuinely necessary.

AGREEMENT BETWEEN PARTICIPANTS

Where electronic documents, especially e-mails, are used in contractual or other commercial arrangements, a framework should be drawn up to regulate the terms, conditions, responsibilities and liabilities of using electronic documents. For business conducted between the MOD and its Industry partners there are a number of standard conditions and model agreements which can be utilised – these are referred to in Annex A.

LEGAL ASPECTS OF USING ELECTRONIC DOCUMENTS

Chapter 2 covers the main issues governing the conduct of e-Commerce. There are a number of statutes and legal issues to bear in mind when using electronic documents and e-mails which, within the MOD, are detailed in JSP700.

The key issues are:

- **Deleting Documents.** Deleting documents is not quite as straightforward as destroying paper documents. On the Microsoft-type operating systems, selecting delete merely places the document in the "delete bin". Even emptying the "delete bin" does not necessarily destroy the document. In many cases they will be retained in back-ups, or may be recoverable from disks and other storage. In certain circumstances, such as criminal investigations or legal action, an organisation may be obliged to search back-ups or other areas to recover "deleted" documents. It is vital therefore to take care with the content of electronic documents and ensure that the contents could be defended if necessary;
- **Data Protection Act.** Any electronic document, including e-mails, containing personal information may have to be released under a subject access request;
- **Freedom of Information Act.** When the Act comes fully into force in 2005, it will establish a general and fully retrospective right of access to any information held. This will include all information in electronic documents and e-mails, including those containing information belonging to Industrial partners, unless disclosure would give rise to an actionable breach of confidence or is otherwise exempt;
- **Copyright, Design and Patents Act 1998.** This applies equally to electronic documents, e-mails and websites as to conventional documents. While copyright provisions are generally well understood, the ease with which electronic material can be accessed, copied and distributed means that it is very easy to breach copyright provisions. It is therefore prudent that electronic documents are properly labelled with the appropriate copyright and other restrictions and legends, and all users take care to comply with them when handling electronic documents and other material.
- **Confidentiality Obligations.** In general, all useful and reusable information supplied between parties, whether orally or in writing (which includes electronic documents) is subject to an express or implied obligation on the recipient not to disclose the information to others and not to use the information for purposes other than for which it was supplied. Ease of copying this information and distributing it by electronic communications raises questions as to whether these are proper actions having regard to the obligation of confidence.

WHO SHOULD I CONTACT TO FIND OUT MORE?

MOD and most of its Industrial partners have information management authorities who should be contacted in the first instance.

ARE THERE ANY BACKGROUND DOCUMENTS?

Within the MOD the Joint Services Publication (JSP) 700 series of documents provide advice on improving the management of electronic documents in general with further guidance on e-mail standards, the deployment and use of EDRMS systems, information held in a shared file store and paper systems and legal aspects of using electronic documents.

JSP441 contains further information on record-keeping policy.

Guidelines For Industry No. 9 contains suggestions on agreeing a framework for using e-mails in commercial relationships.

Guidelines For Industry No. 15 (Issue 2) covers the commercial considerations of using SWEs.

Guidelines 9 and 15 can both be found under "GFI" of web site:-

<http://www.ams.mod.uk/ams/content/docs/toolkit/ams/admin/navigation/frames.htm>

Sustainable electronic records: strategies for the maintenance and preservation of electronic records and documents in the transition to 2004, Public Record Office, viewable at:

www.pro.gov.uk/recordsmanagement/eros/preservation_toolkit.pdf

CHAPTER 4

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

WHAT IS THIS CHAPTER ABOUT?

This Chapter is about identity management – how, in an environment where information is being accessed or shared across organisations, each organisation can be confident that the people involved are who they say they are. Without this, there is no basis for trust. The provision of identity warranting and management schemes through technical, operational, policy and legal controls is an essential requirement for conducting e-Business in a secure and commercially sound manner.

KEY POINTS

- Electronic signatures are legally admissible and, when taking the form of a Digital Signature generated and subsequently managed by a trusted Public Key Infrastructure, can provide a high degree of assurance in the identity of users;
- Registration Authorities are responsible for checking the proof of identity of users requesting certificates, but not for the data content of messages subsequently created by those users;
- MOD has established its own Root Authority for MOD employees within Government networks. A commercial Root Authority, with associated CAs and RAs, has also been implemented by the MOD for interactions with its trading partners.

DETAIL

THE LAW & PKI

English law now permits any parties involved in a commercial arrangement to use almost any mutually agreed form of electronic or written form of signature as an indication of identity and authority. The advent of widespread and international electronic business demands a standard electronic mechanism for trusted identification, managed at the corporate level, or higher. The most common approach is a Public Key Infrastructure (PKI), which encompasses the means of establishing and then proving identity and the cross-organisational management and technical mechanisms for ensuring that the means of proving identity remain trustworthy at all times.

PUBLIC KEY INFRASTRUCTURE

A user wishing to register for a public key certificate will contact a Registration Authority (RA) associated with the PKI. The main role of the RA is to check the identity of the requesting user against a predefined set of Proof Of Identity (POI) criteria. In many cases there will be a range of different POI criteria, each corresponding to establishing a different level of trust. As a general rule, the higher the level of trust required, the more stringent the checking that will need to be performed.

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

Details of the required levels of checking as well as specific responsibilities, obligations and liabilities associated with each trust level will be documented in a Certificate Policy (CP). The CP will also provide details on how the public/private key pair will be generated, stored and managed. For example, where a high level of trust is required, the private key may be generated and stored within hardware tokens such as a smartcard.

Finally, a technical certification request will be generated that links the user's public key to information about the user. This information will usually include the identity of the user. The RA will also include other information within this request, including a reference to the specific CP that will apply. The request will then be digitally signed by the associated private key and passed to the Certification Authority (CA).

The CA will check the integrity of the certificate request by ensuring that the public key in the request is linked to the private key used to digitally sign the request. Providing this is correct, the information held in the request will be used to create a new public key certificate. The public key certificate is now ready to be used by the user.

Where the certificate includes details about the user's identity it may be used as an additional proof of identity, in many respects like a paper passport. A third party receiving a digitally signed message from a user can use this certificate to check whether the sender possesses the corresponding private key. If they do, and the certificate is valid and from a trustworthy PKI, then they know that the certificate 'belongs' to that user and therefore the information in that the certificate relates to them.

In general terms, a digital certificate may be used for a number of different security-related purposes. The CP used by the RA will include details on which security services are supported. These so-called 'key usage' details will be included within the certificate itself.

Possible security services that can be supported by certificates include:

- | | |
|------------------------|---|
| Authentication | The ability to check that a sender of a message is who they claim to be. That is, the sender is in possession of the private key that matches the public key certificate they send with the message. If it does, then they are the user identified in the certificate. |
| Integrity | The ability to check whether or not a message or attachment has been altered since it was digitally signed (by the sender). |
| Confidentiality | The ability to protect information using the recipient's public key to encrypt it, so that only the holder of the private key (the recipient) may decipher it and recover the original information. |
| Non-Repudiation | A public key certificate can be used to show that information has not been altered since it was sent, and that the sender corresponds to the identity shown in the public key certificate. These two functions may be used as part of the provision of a non-repudiation service. |

Note that there may be requirements for additional technical, policy, legal and operational controls in order to strengthen the possible evidentiary weight associated with any data collected.

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

MESSAGE ASSURANCE REQUIREMENTS

In general, the recipient of an electronically sent message wants to know who sent it, whether the content has been deliberately or inadvertently altered after leaving the sender, and that it could only have come from the sender (**integrity**).

Depending upon the nature of the communication, the sender may also wish to ensure that only the intended recipient can read the message (**confidentiality**).

Finally, the sender may wish to gather evidence that the message was successfully delivered, which the recipient cannot later deny (**non-repudiation**). Note that the recipient may also wish to gather evidence that supports the case that the message was sent by the sender at a specific date and time.

For postal mail, the sender's hand-written signature can be taken as proof of message authenticity. The difficulty in making an undetected change to hardcopy provides sufficient assurance of integrity. The use of registered mail, by collecting the recipient's own signature as confirmation of delivery, provides non-repudiation.

Parties should also be able to communicate reliably with each other, with confidence that their identities are established, with neither party being impersonated, and with an assurance that communication cannot be repudiated.

MEANS TO ACHIEVE ELECTRONIC MESSAGE ASSURANCE

Companies has been exchanging data electronically for years using Electronic Data Interchange (EDI) connected over Value Added Networks (VANs). These member-only networks provided message assurance by behaving as the equivalent of a trusted courier service. Major corporations adopted EDI but it has not found favour with smaller companies, mainly on cost grounds. Conversely, the Internet has a comparatively low entry cost, but provides none of the value-add implicit in VANs. Alternative mechanisms to provide message assurance are required.

ELECTRONIC SIGNATURES

A digital signature can be considered as an equivalent of a hand-written signature, when it is supported by appropriate policies and practices. If a digital signature can be inextricably bound to a message, it can be used to provide an assurance that the message has not been altered and that the sender is the user identified by the corresponding certificate. This assurance can be derived from using the certificate and its associated public key to ensure that the sender is in possession of the correct private key and that the certificate is still valid (not expired, suspended or revoked). In addition, a check can and should be performed to ensure that any usage conditions specified in the appropriate CP have been adhered to.

Multiple technologies exist to create an electronic signature of this sort. The European Electronic Signatures Directive, which provides a common framework for electronic signatures, is technology neutral. However, the Directive is largely based on the use of asymmetric encryption (using Public and Private Key pairs) and certificate-based verification, which are characteristics of Public Key Infrastructure (PKI) - the most common example of digital signature technology.

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

THE EUROPEAN ELECTRONIC SIGNATURES DIRECTIVE

The European Electronic Signatures Directive (submitted by the European Commission in May 1998, in law from July 2001) provides a common framework for electronic signatures. This includes a legal framework. As a general principle, the Directive states that Member States may not deny the legal effect of an electronic signature merely because of the electronic form of the signature.

A second principle of the Directive is that Member States are obliged to recognise certain types of electronic signature as having the same legal effect as they would give to hand-written signatures. This second guarantee only applies to "advanced" electronic signatures which are based on a "qualified" certificate and which are created by a "secure" signature creation device. For qualified certificates, the Directive is not technology neutral: it mandates certificate-based asymmetric cryptography and CAs.

The Directive thus provides two levels of legal certainty for electronic signatures depending on the level of technical security relating to the signature. On the first level, electronic signatures in general cannot be denied legal effect. On the second level, electronic signatures filling certain technical security requirements (as defined in the Directive) will have same legal effect as hand-written signatures.

The Directive also establishes a minimum liability regime for Certificate Services Providers (CSPs) issuing qualified certificates to the public. Member States are obliged to ensure that such CSPs are liable for damage caused to a person who reasonably relies on the certificate. The Directive allows CSPs to indicate limits on the uses of certificates and the value of transactions for which the certificates can be used. The CSP is not to be liable for damages arising from contrary use of a qualified certificate, which includes limits on its use.

THE UK ELECTRONIC COMMUNICATIONS ACT

In May 2000, the UK Electronic Communications Act (ECA 2000) was passed. This defines any electronic signature as anything in electronic form incorporated into a communication or data to establish the authenticity or integrity of the communications or data. An electronic signature is admissible in evidence in relation to any question as to the authenticity of the communication or data or as to the integrity of the communication or data.

ECA 2000 does not, however, fully implement the Electronic Signatures Directive in that it does not deal with:

- a) The enhanced protection for advanced electronic signatures as defined in the Directive or;
- b) Certificate services providers (service provision based on CAs and RAs) and, in particular, the provisions of the Directive relating to the liability of CSPs who issue qualified certificates.

The Government has supported the initiative of the Alliance for Electronic Business in setting up a voluntary self-approvals scheme (tScheme) for the regulation of the CSP marketplace. A number of Approval Profiles are published, describing how CSPs should operate specific 'trust services' in order to attain tScheme approved status. CSPs are assessed for compliance against these profiles by a number of UKAS accredited assessors, who recommend to tScheme whether or not approval should be granted and how long before a reassessment of the trust service will be required.

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

LIABILITY

A CSP takes responsibility for issuing digital identities to individuals who have met authentication pre-requisites, and for revoking users on receipt of valid notification. For example, the Certificate Policy that applies to the certificate may require a telephone call from a known user followed by a written letter of confirmation. A CSP will be expected to accept limited liability, to cover failure of the registration and issuing processes within its control. For example, where a certificate is issued to a user that has not supplied valid proof of identity information (as defined within the appropriate CP) during the registration process.

Importantly, the CSP does not warrant the original data/information secured using a certificate – the ECA 2000 does not require this. The lack of case law in this area however, results in a corresponding lack of clarity regarding what is a reasonable level of liability in the event of damage caused by an incorrectly issued certificate being used as part of a high-value transaction.

UK PKI & TRUST MODELS

MOD SITUATION

To avoid potential issues of liability, the MOD has adopted the strategy that industry partners should use certificates issued by commercial CAs, whereas MOD personnel should use certificates issued by MOD CAs. To this end, the MOD has created a top-level CA (known as a Root CA) under which subordinate CAs can be created to issue certificates to MOD personnel.

DECS SITUATION

DECS trading partners will use commercially issued certificates, whilst MOD users will be using both MOD certificates internally and commercially issued certificates externally. Realisation of the MOD policy therefore creates a minimum of two separate communities of DECS users. Conceptually, to establish trust between these communities there are two options: global trust in which a direct relationship is established at CA level (for example cross-certification in which CAs establish parity of trust) or local trust in which each business application is configured with the list of CAs which it should trust. The former option is primarily suited to internal CAs within hierarchical organisations. The latter option is more suited to inter-organisational trust, and is the intended approach for DECS.

A PKI simply provides the capability to check the identity of a user, register their identity within a public key certificate that is tightly bound to a specific public key and check that the user has access to the corresponding private key. It doesn't "do" anything with the certificates. To use certificates, application software, capable of signing and verifying certificates, is required. This is sometimes referred to as being 'PKI Enabled'. Ideally, all application software would provide these functions as a matter of routine, but this is currently not the case - although it is improving.

The initial requirement for PKI on DECS is for the authentication of users accessing DECS over the Internet. The PKI "aware" software being used for authentication is Novell's iChain product set. ChamberSign, an initiative of the British Chambers of Commerce that has been granted tScheme approval, has been selected as the preferred CSP for the provision of DECS authentication certificates.

PUBLIC KEY INFRASTRUCTURE AND ELECTRONIC SIGNATURES

It is anticipated that the use of certificates for message assurance (e.g. e-Procurement, e-Tendering) will be implemented as and when the specific business requirements are articulated and accepted, and when suitable PKI enabled application software becomes available.

EUROPEAN PKI INITIATIVES

Other European nations have emerging Government PKI initiatives for internal use. Chambersign is perhaps the most relevant commercially available PKI in the context of the MOD and DECS, as it is backed by most European Chambers of Commerce, membership of which is mandatory in several European countries, e.g. Italy and France.

ChamberSign is an initiative set up by Chamber of Commerce organisations of 10 European countries and Eurochambres, which aims to create a comprehensive architecture for secure business-to-business electronic commerce across international borders. ChamberSign is starting to make access to digital signature technology more widely available to the business community and is achieving international recognition and interoperability of digital certificates issued by Chambers of Commerce. ChamberSign covers the territories of Austria, Belgium, France, Germany, Italy, Luxembourg, the Netherlands, Spain, Sweden and the United Kingdom. Further expansion of the network is being planned to include nations worldwide. Involvement with the USA is an early goal.

US SITUATION

The PKI situation in the USA is both the most advanced and most complex. Many corporations have identity management initiatives. Exchanges are starting to offer various types of identity management services, including PKI. However, it is the US Federal Government community that is most advanced:

β US DOD External Certificate Authorities (ECA) provide certification services for industry. <http://www.disa.mil/infosec/pkieca/documents.html>

β US Federal Bridge Certificate Authority (FBCA) programme is in the early stages of providing a bridging mechanism for all Federal Government departments. One of the options being considered is to link the ECA into the FBCA, thus providing a trust path between industry and the Federal environment. If this is agreed, then there may also be an opportunity for approved US/UK corporate PKI communities to be linked to the Federal Bridge. <http://www.cio.gov/fbca>

SUMMARY

Any company or organisation that wants to engage in cross-organisational information sharing or e-business will need to address identity warranting and management. Public Key Infrastructure is an essential tool for the secure conduct of commercial activities by electronic communication, providing a structure for authentication, non-repudiation and digital signatures.

ARE THERE ANY BACKGROUND DOCUMENTS?

Planning for PKI: best practices guide for deploying public key infrastructures.
Housley & Polk. Wiley. ISBN 0471397024

The European Electronic Signatures Directive
http://www.bc.edu/bc_org/avp/law/lwsch/journals/bciclr/24_1/04_TXT.htm

Electronic Communications Act 2000
<http://www.hmso.gov.uk/acts/acts2000/20000007.htm>

Further information on ChamberSign is available from Eurochambres at
<http://www.eurochambres.be/whatwedo/chambersign.htm>.

[Insert further SIs eg The Electronic Commerce (EC Directive) Regulations 2002, No 2013]

CHAPTER 5

THE DEFENCE ELECTRONIC COMMERCE SERVICE (DECS)

WHAT IS THIS CHAPTER ABOUT?

This chapter describes the Defence Electronic Commerce Service and summarises the role of DECS and the arrangements between MOD and Cap Gemini Ernst & Young (CGE&Y).

KEY POINTS

- DECS is a long-term Public/Private Partnership between MOD and CGE&Y;
- DECS is an enabling platform for hosting a variety of e-commerce and business services;
- The DECS platform can also be utilised by MOD's Trading Partners (TPs) for hosting Business to Business services;
- DECS is a MOD-wide initiative: it is not limited to Defence Logistics Organisation business;
- DECS is here now – the MOD's electronic purchasing (see Chapter 6) is conducted over the DECS platform and a Shared Working Environment is available to MOD and industry through DECS.

DETAIL

WHAT IS DECS?

DECS VISION

A partnering arrangement between CGE&Y, MOD and Industry to enable Defence to drive down costs through the delivery of world-beating business services.

DECS MISSION

To enable MOD and Industry to achieve efficiency savings and improve capabilities through the delivery of application services and guidance on best commercial practice.

STRATEGIC OBJECTIVES

- 1 To deliver services that:
 - deliver value for money to MOD and its suppliers
 - enable MOD and its suppliers to achieve increased efficiencies and savings
 - the DECS design and infrastructure investment
- 2 To propose ways in which the MOD, other government departments (OGDs) and Trading Partners can maximise benefit from DECS capabilities.
- 3 To seek operational efficiencies and continuous improvement in the delivery of DECS services.
- 4 Become an integrated, high-performing team that effectively manages the delivery and exploitation of DECS capabilities.
- 5 To ensure that DECS capabilities are exploited across the whole of the defence community.

THE DEFENCE ELECTRONIC COMMERCE SERVICE (DECS)

THE CONTRACT

The DECS Contract is a ten year Public/Private Partnership between MOD and CGE&Y, with an option to extend to up to fifteen years in total. It was launched in July 2000 by then Defence Minister John Spellar. The contract is managed by the DCSA CBA/IPT on behalf of the DLO and the Senior Responsible Owner is Director General Strategic & Logistic Development.

PURPOSE

DECS is a key enabler in the creation of a Defence Community e-Business environment by providing an e-business hub to allow the incremental addition of future services to meet both MoD and trading partner requirements. This will ensure that DECS rapidly evolves into an e-Business environment where information is shared collaboratively for the mutual benefit of MOD and its trading partners.

The Defence Logistics Organisation (DLO), created to bring together the three separate armed forces logistics organisations, and with an overall budget of around £5 billion per annum, regards DECS as essential to achieving its efficiency targets. The Defence Procurement Agency is also a key stakeholder and will become a significant user of the SWE and future collaborative working services.

CONNECTIVITY

The DECS Platform is a physical realisation which has been specifically designed to meet the requirements of a complex and secure business environment. Connection to the DECS Platform is available via the MOD's Restricted LAN Interconnect, the Internet, Value Added Networks (IBM, BT and AT&T) and EXOSTAR (a major electronic marketplace created for the aerospace sector). DECS enables the MOD's trading partners to interact with the MOD using a range of technologies, including web browser and Electronic Data Interchange (EDI). This allows individual trading partners to select the method of communication most suited to their business needs.

SECURITY STANDARDS

Security and confidentiality are prerequisites for utilising electronic communications in the Defence sector. This applies not just to issues of national security, but also to the protection of intellectual property and commercially sensitive material. DECS complies with the MOD security requirements, as outlined in JSP 440 - the Manual of Protective Security – and also provides rigorous but pragmatic solutions for ensuring commercial privacy which reflect best commercial practice.

ALTERNATIVES TO DECS

Whilst DECS is the main platform through which the MOD securely connects with industry, there are various alternatives for both MOD IPTs and Industry. One such Government-approved supplier already delivering secure collaborative working solutions (SWE) for critical projects in the aerospace and defence sector, including MOD IPTs, is UltraSBS. Their solutions can be delivered over the RLI and developed to meet the specific needs of individual IPTs.

THE DEFENCE ELECTRONIC COMMERCE SERVICE (DECS)

SUMMARY

DECS provides MOD and its trading partners with opportunities to work collaboratively, and to drive out inefficiencies in pursuit of mutual benefit.

WHO SHOULD I CONTACT IF I WANT TO FIND OUT MORE?

For further information contact the DECS service desk

Tel: **0870 241 3569**

E-mail: decs.servicedesk@cgey.com

For further Information, on UltraSBS, contact:

Marie McCarthy

Tel: **01772 325290**

E-mail: information@ultrasbs.com

Website: www.ultrasbs.com

ARE THERE ANY BACKGROUND DOCUMENTS?

The DECS website can be accessed at www.d2btrade.com.

CHAPTER 6

PURCHASING

WHAT IS THIS CHAPTER ABOUT?

This Chapter explains how the Ministry of Defence is introducing electronic purchasing via its Purchase to Payment (P2P) project, and outlines the effects upon Industrial relationships. Unlike some other chapters, where the solutions are perhaps more varied, this chapter is focused around a real MOD project, deliverable a specific capability and is therefore more practically based.

Key points:

- P2P enables electronic ordering, receipting and invoicing;
- P2P is intended to be an MOD-wide system, but initially will be implemented in the Defence Logistics Organisation (DLO);
- Electronic purchasing can provide improved cash flow predictability;
- P2P provides improved linkage of purchasing to financial management;
- MOD can utilise P2P to identify purchasing trends and better management information.

DETAIL

WHAT IS P2P?

P2P utilises an Oracle system based on standard commercial practice, which will allow the MOD initially to trade electronically, i.e. by electronic communications, with its Industrial partners via the Defence Electronic Commerce Service (DECS). It will ensure a timelier and more cost-effective procurement process, and will be used for the purchase and payment of services and goods (inventory and non-inventory). The intention is that P2P will become the electronic purchasing⁴ system for the whole of the MOD.

HOW WILL THIS AFFECT THOSE INVOLVED IN PURCHASING?

The P2P initiative will enable:

- An electronic order for goods and services to be sent to a Trading Partner;
- An electronic receipt to be held and linked to the order for goods and services;
- An electronic invoice to be sent to the MOD;
- The order, receipt and invoice to be matched on-line, generating an electronic message authorising the DBA to process the payment to the Trading Partner;
- The Defence Financial Management System (DFMS) to be updated with the necessary information.

⁴Purchasing refers to the transactional activity carried out under the aegis of contracts, which are the overarching legally binding agreements between parties. P2P does not, as currently constituted, embrace the placing or management of contracts, and therefore may not necessarily be applied to some larger, more complex contracts which involve little transactional activity.

When P2P is deployed, those involved in purchasing on behalf of the MOD will assume new roles and responsibilities, for which they will receive training. For example, the Defence Bills Agency will perform the Accounts Payable function in lieu of their current price-matching responsibilities, which will now be performed by P2P.

WHAT IS THE IMPACT ON INDUSTRY?

There are a number of benefits to Industry in the P2P initiative, the main ones being:-

- An The commercial processes employed should enable Industry (described on P2P as Trading Partners (TPs)) to work with MOD in a similar manner to their other customers, i.e. they will no longer have to configure their business processes and information systems to work in a MOD-specific manner.
- An The automation of processes should speed up doing business with the MOD.
- An TPs should find improvements to cash-flow predictability.

COSTS TO TPS.

As originally envisaged,TPs would have been charged for access to the DECS-hosted purchasing service. However, in the better interests of Industrial partners, the MOD has decided to bear these costs itself. As well as demonstrating the Department’s commitment to e-Commerce, this should also encourage all of the MOD’s Industrial partners over time to use the facility.

Whilst there are to be no joining or transaction costs to the TP, enabling connection to DECS may incur ‘back office’ costs. These will be the responsibility of the TP.

Finally, dependant upon the connectivity option chosen, there may be some associated costs to TPs. The following diagram gives an indication of what these costs might be, although it should be borne in mind that they could be more or less than those illustrated and there may be additional options to fulfil these requirements.

	EDI	Internet DECS Purchasing Portal	Web browser software is required Exostar SupplyPass
Set up Charges	Kewill EasyTrade £1350 one-off charge, which includes software, based on a single-user installation trading with the MOD only. Other Industrial partners will vary	Purchase of card reader for PKI smartcards from ChamberCard - £106 per reader.	\$250 one-off set-up fee MAY BE REQUIRED: Purchase of card reader for PKI smartcards. Charges to be advised.
Annual Charges	Kewill EasyTrade £420 based on a single-user installation trading with the MOD only. Other Industrial partners will vary.	Digital certificate for each individual user from ChamberSign - £70 per annum, paid upfront for three years	\$1600 per annum for DECS connection \$395 per annum Exostar subscription. MAY BE REQUIRED: Digital certificate for each individual user. Charges to be advised.
User Training	Included in the one-off charge	Downloadable training materials in development. Charge, if any, to be determined	Free seminars covering the use of SupplyPass for Exostar subscribers, plus downloadable self-training materials

Please note that all of these costs are indicative and may be subject to revision

Migration of Suppliers to P2P. Cap Gemini Ernst & Young (CGEY), the DECS service provider, is responsible for migration of existing suppliers to P2P, in line with MOD instructions.

Existing contractual arrangements will need to be migrated to the new business process. This can only be achieved, by agreement with Industry, through the amendment of the contracts. All Industrial partners identified for possible migration to P2P should therefore expect to receive a letter, either from MOD or from CGEY acting on MOD's behalf, giving them reasonable notice of the department's intent to migrate business to P2P. This will be followed up by further information and communications events. Note, however, that as the take on the TPs must align with the roll out of P2P within the department, not all Industrial partners will receive letters immediately.

SUMMARY

P2P will revolutionise the way that the MOD conducts purchasing. By taking this step MOD has enabled business to be conducted in the electronic environment. Benefits to MOD and Industry alike include a reduction in the current large amounts of paperwork, a decrease in the purchasing cycle time-scale through increasing automation of the process, and improved certainty of cash-flow.

WHO SHOULD I CONTACT IF I WANT TO FIND OUT MORE?

DECS Service Desk (DECS & the registration process);

Tel: **0870 241 3569**

E-mail: decs.servicedesk@cgey.com

Further advice on MOD's commercial policy on P2P:

Gwen Beale,
Principal Directorate Commercial,
DLO

Tel: **01225 467530**

E-mail: [-](#)

ARE THERE ANY BACKGROUND DOCUMENTS?

General Information on DECS and P2P - DECS

Website: www.d2btrade.com

DCTM 17/2002 – Electronic Purchasing for the Defence Logistics Organisation

DLO/DECS Purchase to Payment intranet site (only accessible from within the MOD)

Website: www.p2p.dii.r.mil.uk

CHAPTER 7

COLLABORATIVE WORKING

WHAT IS THIS CHAPTER ABOUT?

This chapter introduces the concept of collaborative working and considers the commercial implications of sharing information within that environment.

Reference in this chapter is made to Shared Working Environments (SWE), the term which is now more generally used for a collaborative working environment. Previously these were referred to as Shared Data Environments (SDE).

KEY POINTS

- Shared Working Environments (SWE) can enable collaborative working;
- The MOD's commercial approach addresses Industry concerns surrounding the concept of collaborative working, in particular those related to Intellectual Property Rights, Confidentiality and Liabilities;
- SWEs are already in use in many parts of the MOD and Industry.

THE DETAIL

COLLABORATIVE WORKING - WHAT IS IT?

In many Industry sectors, the focus of collaborative working is on the manufacturing and delivery of physical projects in a lean supply chain. Although this aspect of collaboration can be found in the production and support phases of the Aerospace and Defence lifecycle, the real gains to be made are in the design and development phases.

In simple terms, collaborative working involves using information systems to enable individuals or groups of individuals to work concurrently on information, no matter whether they are dispersed or co-located. There are a number of system approaches to achieve this, but this section will focus primarily on SWEs.

An SWE is a secure electronic environment created to facilitate authorised access to, and communication of, information. The content may be anything the contributors require it to be but typically may consist of all types of documents, databases, background information and the like. It could be thought of as a private electronic website or club (although it may not necessarily be connected to the internet). SWEs are sometimes referred to as Collaborative or Co-operative Working Environments, but don't be confused by the terminology - all these terms basically mean the same thing: a secure electronic community of interest.

Collaborative working can be a powerful tool for project teams, and many of the MOD's Integrated Project Teams (IPTs) have already established SWEs with their industry partners, which are realising business benefits.

WHY COLLABORATE?

Collaboration is becoming an increasingly important element of designing, building and supporting complex systems exemplified by the aircraft, ships and vehicles supplied by industry for use within the MOD. Collaboration is driven by both the complexity itself, which means that a number of specialised sets of skills and knowledge are required to deliver the end product, and by pressure from customers for better, faster, cheaper delivery – a key tenet of the SMART acquisition philosophy.

Sharing data and information is a vital component of a true collaborative relationship, enabling:

- those collaborating to add value to data and information by sharing their insights and ideas, discussing options, and raising questions;
- members of the team to share activities and actions, and track progress;
- people to organise and search for information more effectively and efficiently;
- all of the above to be carried out in a highly secure environment.

However, the sharing of information alone does not address the many other aspects of collaboration that are necessary to reap the maximum benefits:

- integrated processes;
- sharing of tacit knowledge and personal insights;
- generation of new and better ideas;
- joint problem-solving;
- joint risk identification; and
- faster learning.

SOME BENEFITS OF COLLABORATION

The benefits generated from collaboration will relate to the nature of the project and vary according to the maturity of the project.

However, some generic benefits may include:

- Shared information and knowledge with a common set of data to manage business decisions;
- Faster access to the latest versions of information across a programme;
- Enables streamlining of business processes;
- Faster communication of shared information;
- Reduction in multiple sources of data (with associated configuration and quality problems) – "write once read many" (WORM) concept;
- Time and cost savings – travel & subsistence, paper, postage, quality time, paper storage capacity.

WHO SHARES?

Participation in a SWE can be open to anybody who has agreed to work collaboratively, subject to the safeguarding of the interests of members of the community. Where a SWE is established in support of an MOD IPT, MOD will of course be a participant, but must be identified according to the constituent parts of the MOD participating, such as the IPT or other parties such as Customer 1 or 2. This ensures that access to information is properly controlled and that it is not used for purposes other than those for which it was provided.

Industry will also participate in SWEs created to support MOD IPTs, and this is not limited only to the Prime Contractor but also sub-contractors, a third party service provider, in fact anyone with a need to share information.

THE COMMERCIAL APPROACH

The handling of commercial considerations, such as intellectual property, liabilities and confidentiality, is key to building successful collaborative relationships. MOD has agreed with Industry representatives a series of commercial documents (detailed below) that provide models for collaborative working. The suite of documents, which includes model contract documentation, is held together by an overarching guidance document, which is accessible via the MOD's Acquisition Management System website (see below for website address). The aim of the approach is to enable organisations (even those who may be in competition with each other) to share information in a secure and commercially protected environment. Fundamental to this approach is the acknowledgement that the mere act of shared access to information does not concede intellectual property rights, nor does it entail exposure to liabilities beyond those enshrined in contracts.

DEFCON 687A – PROVISION OF A SHARED DATA ENVIRONMENT SERVICE

- Defines the standard contractual responsibilities of any party contracted to supply an SWE service;
- The service provider can be a Prime Contractor or a specialist third party;
- Any variables to be detailed in the contract schedule of requirements (a model is currently being developed);
- The SWE can be a centralised database or a federation of systems – or a mix of both;
- The DEFCON is broadly applicable to any technical or commercial model;
- Since the DEFCON is a standard, it will enable users of a service to understand the crucial elements of the contractual relationship to establish the service, without requiring access to the contract itself;
- Should not be modified or caveated unless absolutely essential.

DEFCON 687B – SHARED DATA ENVIRONMENT SYSTEM TRANSFER ARRANGEMENTS

- Covers licensing arrangements for continued usage of the system at conclusion of the contract where anything other than standard configuration of Commercial Off The Shelf (COTS) products is deployed, e.g. where the service provider has an intellectual property right in the application;
- Should not be modified or caveated unless absolutely essential.

DEFFORM 687C – ELECTRONIC INFORMATION SHARING AGREEMENT (EISA)

- Is a drafting template (and can therefore be varied to address project specifics) but is robust enough to be used without amendment;
- Defines the mutual rights and responsibilities of all users of an SWE service;
- Service Provider must be a signatory;
- Once signed, the EISA is a legally binding agreement;
- States that provision of information into an SWE implies no transfer or granting of IP rights;
- No liability inferred by sharing information – any liabilities must be addressed in underlying contracts;
- *The EISA binds all users to:*
 - Ensure staff are properly authenticated;
 - Observe access control arrangements;
 - Mark information correctly;
 - Provide information in the correct format;
 - Protect information.
- *Users have rights to:*
 - Withdraw their own information;
 - Withdraw from the SWE (excludes the MOD and the service provider);
 - Control access permissions to their own information;
 - Request an "integrity" audit of the system.
- Relies on a separate protocol document for the detail of the client interface;
- The EISA does not add or detract from other contractual responsibilities of the participants

THE RELATIONSHIP APPROACH

While DEFCON 687 provides the commercial framework, the greatest barrier to profitable collaboration remains one of establishing a partnering culture at the management and working levels. The sharing of project, commercial and technical information, particularly in the early phases of a programme, will raise many issues and to enter into a collaborative agreement without addressing them will jeopardise the potential benefits.

The most successful collaborations will involve a network of Customer One, Customer Two, Prime Contractors and Key Suppliers. The dynamics of the team and the information they must share will always present a challenge and a trusted, robust means of addressing that challenge has been jointly endorsed by the MOD and industry.

The aerospace industry uses the Supply Chain Relationships in Action (SCRIA) framework to create step changes in Customer-Supplier relationships and the MOD has subsequently adopted it for use in the SMART acquisition programme. Based on a set of guiding principles and associated code of conduct, SCRIA provides an excellent means of precipitating constructive dialogue with a view to collaborative working. The framework has recently been revised to provide a natural transition into the realms of e-collaboration and Shared Working Environments.

Details of the SCRIA process can be found on the MOD Acquisition Management System and the SBAC website.

SUMMARY

Collaborative working through participation in SWEs can be an effective enabler for driving out inefficiencies and improving business processes. The commercial approach outlined above enables MOD and Defence Industry to participate in SWEs in the confidence that their information is protected, intellectual property rights are safeguarded and they are not exposed to additional liabilities.

WHO SHOULD I CONTACT IF I WANT TO FIND OUT MORE?

Gwen Beale,
Principal Directorate Commercial,
DLO

Tel: **01225 467530**
E-mail: pdc-comm@a.dii.mod.uk

Simon Dunford,
United Kingdom Council for e-Business (UKCeB)

Tel: **0117 9790885**
E-mail: simon.dunford@jctf.org.uk

Nick Stroud,
Enterprise Integration Programme Coherence Team (EPCT),
MOD

Tel: **01225 467879**
E-mail: pct1@a.dii.mod.uk

Defence Procurement Management Training
(who run Information Sharing Seminars, open to MOD and Industry participants)

Tel: **0117 969 0846**
E-mail: dpmt@dpa.mod.uk

ARE THERE ANY BACKGROUND DOCUMENTS?

Guidelines for Industry No. 15 (Issue 2)

Website: <http://www.ams.mod.uk/ams/content/docs/toolkit/ams/admin/navigation/frames.htm>

CHAPTER 8

e-TENDERING

WHAT IS THIS CHAPTER ABOUT?

This Chapter explains what electronic tendering is and what is involved in undertaking it.

KEY POINTS

- E-Tendering can provide for:
 - Faster better exchange of information;
 - Increased security and integrity of tendering;
 - Automation of the evaluation process;
- MOD encourages the use of e-Tendering for some competitions, but the ability to do so is not yet widespread throughout the Department or Industry;
- MOD aspires to introduce a corporate capability to undertake e-Tendering, which ideally will be a Government-wide system.

THE DETAIL

WHAT IS E-TENDERING?

The exchange of information by digital files and electronic communications has been normal practice within the Defence Sector for some time; indeed, tender documentation has often been supported by the use of floppy disks, CD-ROMs or even, in some cases, E-mails. However e-Tendering is more fundamental. It is the conduct of the complete tendering exercise from the advertising of the requirement through to the placing of the contract, including the exchange of all relevant documentation all by electronic communication. Ultimately, contract management and the monitoring of contract performance will be conducted by electronic communications – which we'll now call "electronically".

THE BENEFITS OF E-TENDERING

In addition to supporting the Government's revised targets for conducting business by electronic communications, there are business benefits for both the MOD and Industry in doing so. The range of benefits continues to expand as business processes are changed to maximise the opportunities that electronic tendering can deliver. Detailed below are the most notable:

- Making the Government easier for Industry to do business with;
- Opportunities to stimulate increased interest in the market, by reducing the burden that tendering to Government can be;
- Efficient and effective electronic interfaces between Industry and the MOD leading to reduced costs and timesaving on both sides;
- Quick and accurate pre-qualification and evaluation which enables the automatic rejection of Industry partners that fail to meet stipulated fixed criteria;

- Opportunity for the transmission of quality information to and from Industry to enable a clearer understanding of the requirements and proposals;
- Opportunity to respond quickly to any questions and points of clarification during the tender period;
- Reductions in the traditionally labour-intensive tasks of receipt, recording and distribution of tender submissions.
- Reducing the paper trail on tendering exercises, reducing costs to the MOD and Industry alike and supporting 'green' issues;
- Providing a clearer audit trail demonstrating integrity;
- Provision of quality management information;
- Improved opportunity for like for like comparisons of qualitative and quantitative information resulting in a faster, more accurate evaluation of tenders;

However, in doing so it is vital that current principles commonly applied in procurement in the Defence Sector are maintained, namely those of confidentiality, fairness and equity. However, care must also be taken to ensure that we do not unintentionally inhibit competition by moving ahead of the ability of our supplier base to operate using e-Tendering.

WHAT TENDERING TASKS CAN BE DONE ELECTRONICALLY

With the improved capability across some areas of the MOD and Industry, it is now possible to enable the electronic conduct of competitive and single tender responses, as well as acceptances and rejections. However, this is subject to the following conditions being satisfied:

- Electronic signatures for documents originating from Industry are created and managed by a Public Key Infrastructure (PKI), backed by a commercial provider that has been approved by the MOD PKI Policy Management Authority;
- Electronic signatures for documents originating from the MOD are created and managed by a Public Key Infrastructure managed or authorised by the MOD PKI Policy Management Authority;
- The security and operating procedures of MOD and Industry internal information systems (IS) are maintained;
- The current principles, and not the entire practice, of the MOD Tender Board are fully replicated, by the use of a "virtual" tender box which restricts access to tenders until after the due date and time for receipt;
- The integrity of stored tender documentation is maintained through the use of an appropriate technical infrastructure.

If these conditions are fully met, the requirement for a paper "master copy" is no longer necessary as there is no legal requirement for paper documentation, provided that electronic information is sufficiently robust to enable it to be produced as evidence. However, discretion should be exercised and factors such as the tender value, familiarity of those involved and experience of e-Tendering should be given due consideration. The requirement for a paper master copy of contracts is likely to remain until confidence in an electronic repository for contracts has been developed.

THE FUTURE FOR ELECTRONIC TENDERING

It is the MOD's aspiration to introduce an e-Tendering solution that will encompass the end-to-end tendering process, including Pre-Qualification Questionnaire, the invitation to tender, managing the tender process through to Contract award, contract management and performance monitoring. MOD is currently developing a User Requirement Document and business case to introduce a facility which, it is hoped, might be provided via a pan-Departmental solution being developed by the OGC.

KEY PRINCIPLES TO CONSIDER WHEN CONDUCTING E-TENDERING

Until corporate solutions become available, the key principles which should be considered when conducting e-Tendering are as follows:

- Security
- Confidentiality
- Integrity
- Authentication
- Equity/ Transparency
- Liability
- Trust
- Business Benefits
- Portability of Data
- Flexible Process
- Future Proofing
- Audit trail
- Affordability
- Compatibility/Interoperability
- Firewalls
- Scalability
- Reliability/Availability

SUMMARY

Whilst it is intended to deploy corporate e-Tendering solutions in the future, e-Tendering may already be undertaken where the local capability exists to do so as described above. However, it remains as important as ever to ensure that all the necessary procedures are followed and a robust audit trail created.

WHO SHOULD I CONTACT IF I WANT TO FIND OUT MORE?

Further guidance on electronic tendering can be obtain from:

Grant Lovett
Principal Directorate Commercial,
DLO

Tel: **01225 467593**
E-mail: pdc-comm@a.dii.mod.uk

Guidance on Tender Board procedures can be obtained from:

Mary Shoobridge,
Commercial Services Group,
MOD

Tel: **0117 9132811**
E-mail: CSG-12@dpa.mod.uk

Guidance on PKI can be obtained from:

Anne McFarlane,
Directorate General Information,
MOD

Tel: **0207 218 0603**
E-mail: info-enabsvcsad@csv8o.modnsc.com

ARE THERE ANY BACKGROUND DOCUMENTS?

DCTM 42/2002 Electronic Tendering

CHAPTER 9

REVERSE AUCTIONS

WHAT IS THIS CHAPTER ABOUT?

This Chapter explains what Reverse Auctions are and what is involved in undertaking one. It also considers the appropriateness of the technique for Defence procurement and the legal considerations.

KEY POINTS

- Reverse auctions are competitions held "on-line", with the bid prices visible to all bidders, unless a ranked auction is held in which bidders only know their rank relative to other bidders, but are not privy to actual bid amounts;
- Simple commodity items or services where the marketplace is highly competitive are most suitable for reverse auctions, yet any item with clearly defined requirements and more than one source of supply should be considered;
- It is essential that advertisements for competitions to be run on a reverse auction basis state this clearly, along with the criteria for selection;
- EU Public Procurement Directives do not currently recognise the technique of reverse auctions, but are being amended to do so.

THE DETAIL

WHAT IS A REVERSE AUCTION?

Reverse Auctions, also known as "on-line bidding", are a means of buying items or services against a published specification where pre-selected Industrial partners are invited to bid in an on-line auction. All bids made during the auction are published anonymously on-line, in the expectation that competitive pressure, when bidders see the prices bid, will force prices lower as the auction proceeds. The exception is ranked auctions in which the bid amounts are not known to other bidders. The auction is time limited, but arrangements maybe put in place to ensure that if a "leading" bid is made very close to the timed completion of the auction further time is provided to allow other bids to ensure that the lowest price is obtained. A contract is then awarded to the lowest bidder based on the terms and conditions published at the outset, during the contractor pre-selection phase of the Reverse Auction.

WHAT ITEMS ARE SUITABLE FOR A REVERSE AUCTION?

Reverse auctions rely on competition driving prices down and it therefore follows that the less complex or specialised the goods or service being procured, the greater the chance for a successful auction. Simple commodity items or services which can be clearly defined and have a wide range of potential Industrial suppliers will be best suited to the auction process. However, in considering the use of reverse auctions, it is important to ensure that the principles underlying the existing procurement process, namely those of confidentiality, fairness and equity are maintained.

ADVERTISING

It is essential that adverts for goods or services where a reverse auction is being considered clearly state:

- That the ultimate selection may be made on the basis of a reverse auction;
- The evaluation criteria, including any weighting between fixed elements and the variable element of price;
- Information on the process itself, including details of any third party service provider;
- Conditions of bidding, including the minimum decrements permitted;
- Equipment/technical issues.

PREPARING FOR A REVERSE AUCTION

It is necessary to select a service provider to assist in the conduct of the auction. The MOD is considering establishing a corporate capability for the conduct of Reverse Auctions, but until this corporate capability becomes available it will be necessary for MOD teams undertaking Reverse Auctions to select a service provider on a project-by-project basis. Therefore, in the interim, advice on identifying a suitable service provider should be sought from DCSA through local IS Sections. For Industry there are a number of potential service providers, an example being Exostar which has the capability.

Prior to conducting an auction it is necessary clearly to state the specification of the goods or services to be acquired and to pre-select Industrial partners. Pre-selection should cover issues such as technical ability, financial viability, previous Industrial supplier history, quality etc. The purchaser must ensure that they are confident that any Industrial supplier taking part in the auction will be able to meet their business commitments should they win the auction. Since it would be unreasonable to conduct further checks or negotiations once the auction commences, this pre-selection process is crucial and should be undertaken with considerable rigour and well before the auction is due to take place.

The terms and conditions that will apply to the prospective contract must be stated at the outset and accepted by all prospective bidders. For overseas Industrial partners, particular attention will be needed to deal with the issues of currency and timing. If the bid is not to be in £ Sterling, the exchange rate will need to be agreed in advance of the auction using an exchange rate calculated in accordance with a pre-agreed mechanism.

The auction, when it takes place, should be conducted on the basis of price only with pre-agreed minimum bid decrements (i.e. reductions in price) that will apply. Other variables (which must be quantifiable, capable of being expressed in figures and percentages and agreed with potential bidders during the preparation for the Reverse Auction) must be fixed at the point the auction begins, but may contribute towards the scores awarded to bids. For example, a bidder who can achieve faster delivery may achieve a higher score if they bid the same price as a bidder who cannot deliver as fast, but these scores must be visible to bidders, along with bid prices. The way in which an auction is to be evaluated must be very clearly explained to prospective bidders before the auction commences.

EU LEGISLATION

The current EU Directives do not address electronic reverse auctions because this concept did not exist as a practical methodology when the Directives were formulated or even when they were last amended. However, the EU Directives do not currently permit iterative or repeat tendering and it is the opinion of some that reverse auctions fall into this category and are therefore not permitted under the current UK implementing Regulations. The Directives are in the course of amendment by the EU and are expected to allow for the auction process and to facilitate e-Procurement generally. It will be some time before this change to the Directives takes place and is introduced into UK by Regulation (likely by mid 2004). Until the law is amended, the utilisation of a reverse auction process should be considered on a case-by-case basis, taking legal advice where appropriate.

SUMMARY

The electronic environment can be used for Reverse Auctions which can facilitate the procurement of goods and services at highly competitive prices. Considerable effort is required in the initial stages of arranging the auction to ensure all those taking part understand the requirement being auctioned, the processes involved, their various responsibilities and commitments if they should win and that the result of the Reverse Auction will lead to a formal contract at the prices quoted on-line. Reverse Auctions are a new way of selecting a supplier and are not a replacement for a contract.

WHO SHOULD I CONTACT IF I WANT TO FIND OUT MORE?

Grant Lovett,
Principal Directorate Commercial
Tel: 01225 467593
E-mail: pdc-comm@a.dii.mod.uk

ARE THERE ANY BACKGROUND DOCUMENTS?

DCTM 39/2002
See also Chapter 12

CHAPTER 9

THE GOVERNMENT PROCUREMENT CARD

WHAT IS THIS CHAPTER ABOUT?

This chapter provides detail about the Government Procurement Card (GPC).

KEY POINTS

The GPC:-

- Is the simplest form of e-Business;
- Replaces bureaucracy with simplicity;
- Leads to improved Management Information.

THE DETAIL

WHAT IS IT?

The Government Procurement Card (GPC) is a payment card issued by a number of banks and used throughout Government. MOD has chosen to use Company Barclaycard as their card supplier. The card takes the form of a plastic card, and looks like a normal credit card and can be used in the same way. It is, however, a VISA charge card and MOD is required to settle the bill every month.

MOD, together with other Government Departments, has been the subject of criticism many times because of its costly purchasing procedures. In 1997 a critical National Audit Office (NAO) report highlighted the enormous cost of procuring low cost items through local purchase procedures. As a result GPC was introduced to eradicate outdated bureaucratic practices for the purchase of low value, low risk, off the shelf items normally costing less than £5000. The GPC is best used as near as possible to the end-user so that, ideally, the person who has the need speaks to the supplier direct, thus ensuring he gets what he requires not what someone else thinks he wants. By giving the cardholder both financial and contractual authority it removes the need to seek individual approvals for each and every purchase.

The provision of this service by the card provider is entirely free of charge to MOD. There is an overarching agreement with VISA that is managed by the Office of Government Commerce (OGC) and the MOD has its own Departmental Agreement with Company Barclaycard. The supplier would have to establish a Merchant Agreement with VISA in order to be able to charge to the GPC, if no current agreement exists. The Merchant Agreement will require the supplier to pay VISA a Merchant's Fee for every transaction; this fee needs to be absorbed within the supplier's prices and is not recoverable separately from MOD.

GPC is a true Government wide initiative and has been endorsed by the Treasury and the NAO. There are currently 30,000 government employees in over 160 Government Departments and Agencies using GPC and it is now recognised as the simplest form of e-Business.

WHAT ARE THE BENEFITS?

The Card replaces bureaucracy with simplicity and has a number of benefits for purchasers:

- *Elimination of the "paper chase"* – no need for individual requisition forms, financial approvals, written purchase orders etc.;
- *Environmentally friendly* – less paperwork means fewer trees cut down to make the paper;
- *Order "on demand"* – goods and services can be ordered when required. The need to hold onto stores is greatly reduced;
- *Accuracy of order* – The purchaser is now in direct contact with the Industrial supplier and can make instant decisions on what to buy;
- *Choice* – There are over 600,000 outlets in the UK that will accept the GPC;
- *One payment* – There is only one consolidated payment to the bank at the end of each month instead of making multiple payments to many Industrial partners. This removes thousands of bills going through to the Miscellaneous Bills section at the Defence Bills Agency (DBA) every month;
- *Prompt payment to Industry* – Industrial partners are normally paid by VISA within 4 days and has the added benefit of contributing to Government's prompt payment target. This may allow the negotiation of better prices with suppliers, although speed of payment will have to be balanced with the cost of the Merchant's Fee payable by the supplier to VISA – MOD is likely to be considered as a normal consumer by some suppliers;
- *Management information* – The banks provide comprehensive management information in an electronic format.

TERMS OF TRADING WHEN USING THE GPC

Transactions under the GPC will be subject to the Sale of Goods Act and the Supply of Goods and Services Act, as appropriate, unless other terms are expressly agreed and made part of the transaction with the supplier.

WHAT ARE THE SAFEGUARDS.

Each cardholder is given a delegation letter that will set out the parameters for card use. The Cardholder is required to keep a transaction log of all purchases made. He will receive a statement from Company Barclaycard detailing all transactions made against his card during that month. He must reconcile his transaction log against the statement. He must then send the reconciled paperwork to his finance branch for retrospective requirement scrutiny and verification. Any discrepancies are either taken up with the Industrial supplier or Company Barclaycard as appropriate. All transactions are visible not just on the statement but also in the Management Information which is provided to TLB/HLBs. As well as paying the one GPC bill, DBA also attributes all transactions to cost centres allowing finance branches to "match" commitments against payments.

Additionally specific controls are built into individual cards that cardholders are unable to change. All cards have an individual (single) transaction limit and a monthly credit limit. If required, certain types of supplier can be blocked using the VISA Merchant Category Code facility that allows cards to be tailored to the needs of an individual purchaser.

CHAPTER 10
THE GOVERNMENT PROCUREMENT CARD

Cardholders are not personally liable for expenditure on their cards. MOD is indemnified by Company Barclaycard's corporate liability insurance for Employee and Third Party (Supplier) fraud. Company Barclaycard will also provide reports on instances of attempted fraud. This is particularly relevant when using GPC over the Internet which is an increasing use of GPC, especially booking flights with the low-cost airlines.

SUMMARY

GPC is providing real benefits to users in terms of processing efficiencies, faster deliveries and, in some cases, lower prices. It is also an important signal of MOD's willingness to change the way it does its business. GPC is MOD's first choice method for conducting Low Value Procurement.

WHO SHOULD I CONTACT TO FIND OUT MORE?

For more details of GPC including, for MOD staff, how to obtain a card, contact the GPC Management Team.

Contact details for the Helpdesk are:

Tel: **01264 383610**

Fax: **01264 383617**

ARE THERE ANY BACKGROUND DOCUMENTS?

More detailed information and guidance on GPC can be found in JSP462 Part 6 Chapter 12.

CHAPTER 11

THE e-BUSINESS REVOLUTION

WHAT IS THIS CHAPTER ABOUT?

This Chapter describes in very broad terms the opportunities which the e-Business revolution could provide for the MOD and Industry. It explains how new technology is enabling the development of radically new business processes and how these can be applied.

THE DETAIL

THE CHANGE

Business-to-consumer (B2c) marketplaces are rapidly emerging on the Internet. Flea markets and print classified ads are being replaced by on-line auctions administered by pioneers like ebay and Yahoo! No one doubts that these new consumer marketplaces and selling models are having a major impact on how we purchase goods and services. At the same time, leading Industries are implementing procurement automation solutions, optimising the corporate purchasing processes.

TRANSFORMING BUSINESS INTO AN E-BUSINESS

A new model for business is taking shape, "e-Business", and it's built on the largest communications network on the planet, the Internet. The competitive issues driving Industries around the world, of all sizes and across all industry sectors, call for nothing less than complete organisational metamorphosis. e-Business is the way Industries are fundamentally changing the way they do business using Internet technologies.

THE INTERNET IS CHANGING EVERYTHING!

... from the way businesses interact with suppliers and serve their customers, to how they manage back-office functions such as accounting, payroll, and human resources. e-Business fundamentally changes the way companies do business using Internet technologies. e-Business is affecting every organisation around the world. Successful companies recognise the opportunities e-Business offers and are transforming themselves into e-Businesses. Companies that are slow to embrace e-Business are facing competitors who threaten their very existence.

Leading organisations are transforming procurement into an e-Business weapon - streamlining processes, empowering employees, analysing corporate data and forging effective relationships with Industry.

OPTIMISING PURCHASING THROUGH E-PROCUREMENT

In order to achieve the results promised by full procurement automation, a comprehensive procurement solution that addresses the needs of employees, Industrial partners, and procurement professionals is required. Employees need easy-to-use, browser-based applications easily to purchase goods and services. There is a need to extend internal process efficiencies to Industry, through

XML-based communication. Procurement professionals need the right tools and information to analyse worldwide procurement spend and supplier performance, as well as to source and select the right Industrial partners.

Market leading internet procurement solutions provides comprehensive support for all of these needs.

- **Comprehensive Purchasing Intelligence** – Out-of-the-box analytical applications ranging from simple internet reports to robust data warehouse-based workbooks help you measure performance and identify the most significant opportunities to save money.
- **Self-Guiding Catalogue** – Enables users to find catalogue items quickly with its powerful text-based search engine rather than forcing users through hierarchy drill downs that typically result in dead ends.
- **Supplier Collaboration** – Web-based applications for supply chain partners access to information ranging from business transaction details to performance statistics, so they can be more efficient and better serve the participants.
- **Global Solution** – Support for multiple languages and currencies for companies of all sizes, with services including implementation, training, and support offered around the clock and around the globe.
- **All Products and Services** – Manage any type of goods or services, including production, administrative, MRO, capital, and many more.

SOME CHALLENGES STILL REMAIN

Internet procurement solutions work well for long-term relationship-based agreements, contracts, and catalogue purchases, but if you're a buyer, how do you find the right supplier in the first place? If you're a supplier, how do you find new customers? How do you initiate the relationship? How do you ensure that the relationship will change along with your needs? How do you determine the right price? What about infrequently ordered goods or services?

Interaction with many buyers and suppliers at any given time is crucial, and yet the cost of point-to-point integration to support all these relationships is prohibitive. How do you reduce the cost of doing business and yet remain nimble and responsive?

ON-LINE MARKETPLACES—PURCHASING THROUGH COMMUNITY E-BUSINESS

On-line marketplaces provide tremendous efficiencies as well as opportunities to solve the remaining procurement challenges. Not only will existing buyer/supplier relationships thrive in these e-Business communities, but new relationships are much easier to initiate. Buyers with demand are efficiently matched to partners with supply, and both are assured that the relationship is initiated at right price, with the right lead time, with the appropriate level of quality, and so on. The interaction is easy to the point that relationships can be created around a single transaction. No longer will companies spend countless days searching for the right supplier or the best sales opportunity. When the need arises for a one-time spot purchase, that need can be quickly and easily fulfilled. When a longer-term relationship is required, the partner can be identified and the relationship initiated through the same process. This eliminates huge headaches for both buyers and suppliers.

Consider many of the inefficient markets which exist today. Companies may carry vast amounts of inventory even when a surplus exists which is more than adequate. Why? Because the supply and

the demand cannot be matched efficiently. On-line marketplaces promise to meet the challenge with capabilities like auctioning, bid management, and spot purchasing.

By virtue of the fact that everyone is connected to the same service, the need for point-to-point integration with each trading partner is eliminated. Buyers and suppliers have one place to go to get transaction details and other vital information. And the more participants, the more efficient the communication.

Keys to a successful on-line marketplace include:

- Open to all buyers and sellers;
- Ability to match the right buyers to the right sellers;
- Content and support for all goods and services;
- Transaction routing and support for industry standard protocols.

ABILITY TO MATCH THE RIGHT BUYERS TO THE RIGHT SELLERS

In order to match the right buyers to the right sellers, traditional purchasing models based on catalogues and contracts are being supplemented with new, Internet-enabled models. While catalogue- and contract-based purchasing work well in relatively stable pricing environments, these models don't work well for commodities with volatile pricing or for situations where a relationship doesn't already exist.

BUYER AUCTIONS AND INTERNET BIDS

A buyer auction or Reverse Auction (see Chapter 9) allows buyers to solicit and manage bids from multiple Industry partners on-line. Different from a conventional auction where terms favour the seller, terms in a Reverse Auction are determined by the buyer. Terms could be centred around price, delivery, quality, service, or some combination of them all.

In addition to defining which elements are most critical, buyers can also determine what information will be visible to the Industry partners who choose to respond. The buyer may choose to let Industry partners see information like the current lead time or best price, and let them bid multiple times right up to the closing moments of the bid process. Buyers may choose to have a public bid where any supplier can respond, or they may limit the bidders to those who meet some defined criteria. A bidders' list may be automatically generated from the supplier registry based on those criteria. Either way, the appropriate Industry partners are notified automatically and they can choose to respond and submit their bids.

Buyers then review supplier responses on-line and award a contract or allow additional rounds of bidding. Awarding a contract could be the first step of several in a long-term business relationship.

SPOT PURCHASING

Spot buying allows companies to purchase quickly from suppliers with whom they have no previous formal relationship. And even if there is an existing relationship, there may not always be a contract or detailed pricing arrangements. A great example is maintenance and repair. You may have a parts supplier that you use regularly, but you simply cannot anticipate what parts you will need and when. In fact, many of the purchases may only occur once. In this case a detailed written contract

may not even make sense – you just need to get the goods or have some service performed quickly, subject to the normal statutory terms e.g. by purchasing under the GPC.

CATALOGUE PURCHASES

Buyers have traditionally negotiated contracts for high volume, repetitive purchases. Contracts are also used to lock in pricing as well as negotiate volume discounts from suppliers. Typically, buyers have catalogues or contracts in place for suppliers with long and established relationships. While spot purchases and buyer auctions are valuable purchasing models, a full service marketplace needs to support traditional catalogue and contract purchases as well.

CONTENT AND SUPPORT FOR ALL GOODS AND SERVICES

An important element for the success of any on-line marketplace is the quality and accessibility of its content. Users naturally congregate to sites which offer rich content and intuitive search tools to access the content easily.

SELF GUIDING SEARCH

Most search engines pursue one of two search strategies to locate an item or commodity – aggregation or indexing. Leading search engines on consumer-oriented sites return an indexed list of websites where the content may be found. While this approach decentralises ownership of the content to the supplier, the user is faced with a multi-step search and different search engines and user interfaces at each supplier's website. The content aggregation approach, on the other hand, centralises content from suppliers into a central repository offering a uniform interface and search technology.

SUMMARY

Today's single-buyer, multi-supplier Internet procurement solutions offer great opportunities for improving traditional purchasing by automating transaction processing and enabling supplier collaboration. However, significant additional purchasing efficiencies can be achieved by streamlining procurement in an on-line community of multiple buyers and suppliers.

A viable electronic marketplace solution requires a fundamental understanding of the impact of Internet applications on buyers' and suppliers' business processes.

WHO SHOULD I CONTACT TO FIND OUT MORE?

UK Online for business:

Website: www.ukonlineforbusiness.gov.uk/cms/template/homepage.jsp?id=61297

The British Chambers of Commerce e-Business Clubs;

Website: www.ebusinessclubs.co.uk

The Society of British Aerospace Companies e-Business Working Group;

Website: www.sbac.co.uk

Office of Government Commerce – e-Commerce Team;

Website: www.ogc.gov.uk/index.asp?id=95

ANNEX A

MOD CONDITIONS AND RELATED GUIDANCE

E-COMMERCE

- Guidelines for Industry 9 – Electronic Mail
- Guidelines for Industry 17 – Electronic Data Interchange

DEFENCE ELECTRONIC COMMERCE SYSTEM (DECS)

- DCTM 31/2001 – Purchasing Solutions Delivered via the Defence Electronic Commerce System (DECS)

E-TENDERING

- DCTM – 42/2002 – Electronic Tendering

REVERSE AUCTIONS

- DCTM 39/2002 – E-Purchasing - Reverse/Electronic Auctions

E-PURCHASING

- DCTM 31/2001 – Purchasing Solutions Delivered via the Defence Electronic Commerce System (DECS)
- DCTM 17/02 – e-Purchasing for the Defence Logistics Organisation

SHARED WORKING ENVIRONMENTS (SWES)

- Guidelines for Industry 15 – Contracting for a Shared Data Environment Service (Issue2)
- DCTM 24/01 – Shared Data Environments

ANNEX B

CONTACT NAMES

Throughout the guide there are contact details for organisations who can provide specific support and advice on the subjects covered. This annex provides contact details for the principal MOD and Industry organisations who are able to advise on these issues.

MOD

Principal Directorate Commercial,
DLOHQ,
Spur 8,
Block E,
Ensleigh,
BATH, BAI 5AB

Simon Lydiard Tel: **01225 467260**
Grant Lovett Tel: **01225 467593**
Stefan Hill Tel: **01225 467637**
Gwen Beale Tel: **01225 467530**
Denise Savage Tel: **01225 468470**
E-mail: pdc-comm@a.dii.mod.uk

Directorate General Information

MOD PKI Management Authority,
Room 843,
St. Giles Court,
LONDON WC2H 8LD

Anne MacFarlane Tel: **020 721 80603**
E-mail: Info-EnabSvcsAD@defence.mod.uk

Assistant Director
(Information Age Government),
Room 831,
St. Giles Court,
LONDON WC2H 8LD

Charly Wason Tel: **020 721 81353**
E-mail: infostrat-iagad@defence.mod.uk

Enterprise Integration Programme
Coherence Team,
Spur 12,
Block A,
Ensleigh,
BATH BAI 5AB

Nick Stroud Tel: **01225 467879**
E-mail: pct1@a.dii.mod.uk

OTHER ORGANISATIONS

UK Council for Electronic
Business Task Force,
1 Gypsy Patch Lane,
Filton,
BRISTOL BS34 8LR

Simon Dunford Tel: **0117 979 0885**
E-mail: simon.dunford@ukceb.org

e-Business Forum,
Confederation of British Industry,
Centre Point,
103 New Oxford Street,
LONDON WC1A 1DU

Susan Daley Tel: **0207 395 8247**
E-mail: susan.daley@cbi.org.uk

Office of the e-Envoy,
1st Floor,
Stockley House,
130 Wilton Road,
LONDON SW1V 1LQ

Tel: **020 7270 3000**
E-mail: info@e-envoy.gsi.gov.uk

Directorate of e-Procurement,
Office of Government Commerce,
Trevelyan House,
Great Peter Street,
LONDON SW1P 2BY

Peter Court Tel: **0207 271 1325**
E-mail: peter.court@ogc.gsi.gov.uk

The Society of British
Aerospace Companies Ltd.,
Duxbury House,
60 Petty France,
Victoria,
LONDON SW1H 9EU.

Jafar Tall Tel: **0207 227 1028**
E-mail: Jafar.Tall@sbac.co.uk

ANNEX C

GLOSSARY OF TERMS

AMS	Acquisition Management System	EPCT	Enterprise Integration Programme Coherence Team
b2b	Business to Business	ERP	Enterprise Resource Planning
BAE	BAE Systems	EU	European Union
BT	British Telecom	FBCA	Federal Bridge Certificate Authority
CA	Certificate Authority	GPC	Government Procurement Card
CBI	Confederation of British Industry	HLB	Higher Level Budget
CD	Compact Disc	HMG	Her Majesty's Government
CD-ROM Memory	Compact Disc - Read Only Memory	IP	Intellectual Property
CGEY	Cap Gemini Ernst & Young	IPR	Intellectual Property Rights
COTS	Commercial Off The Shelf	IPT	Integrated Project team
CP	Certificate Policy	JSP	Joint Services Publication
CSG	Commercial Services Group	LAN	Local Area Network
CSP	Certificate Services Providers	MOD	Ministry of Defence
Customer 1	Responsible for developing and managing a balanced and affordable equipment programme from concept to deployment	NAO	National Audit Office
Customer 2	Responsible for using the capability provided by a particular equipment	NPPO	Non Project Procurement Office
DBA	Defence Bills Agency	OEM	Original Equipment Manufacturer
DCTM	Defence Contracts Temporary Memorandum	OGC	Office of Government Commerce
DECS	Defence Electronic Commerce Service	P2P	Purchase to Payment
DEFCON	Defence Contract Conditions	PFI	Private Finance Initiative
DGInfo	Director General Information	PKI	Public Key Infrastructure
DII	Defence Information Infrastructure	PP	Public Private Initiative
DLO	Defence Logistics Organisation	QA	Quality Assurance
DPA	Defence Procurement Agency	RA	Registration Authority
DPA	Data Protection Act	RLI	RESTRICTED LAN Interconnect
DTI	Department of Trade and Industry	SE	Synthetic Environment
ECA	Electronic Communications Act	SWE	Shared Working Environment
ECA	External Certificate Authorities	TLB	Top Level Budget
EDI	Electronic Data Interchange	TP	Trading Partners
EDRMS	Electronic Document and Record Management System	UK	United Kingdom
EISA	Electronic Information Sharing Agreement	UKCeB	United Kingdom Council for Electronic Business
		VAN	Value Added Network
		VAT	Value Added Tax
		WORM	Write Once Read Many