STATE OF THE ART REPORT

VOLUME I

CASE STUDIES ON EUROPEAN ELECTRONIC PUBLIC PROCUREMENT PROJECTS

JULY 2004

Produced by EUROPEAN DYNAMICS S.A.

on behalf of the EUROPEAN COMMISSION

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from his or their legal representative.

Executive Summary

The current report is an outcome of the Public eProcurement project of the IDA (Interchange of Data between Administrations), an initiative of the European Commission. The objective is to analyse existing eProcurement initiatives in Europe, in order to assess the state of the art in electronic public procurement. The objective of this report is to **present the status of eProcurement and deduce eProcurement Practices from reviewed eProcurement systems across Europe** , identifying interesting approaches when reviewing / examining various European systems.

The report is consolidated in two documents (Volumes). Volume I contains the results of the analysis, namely the eProcurement Practices, whereas Volume II includes all background information that was collected during the analysis. In total, **seven missions to European public administrations** have been carried out. The analysis included **21 eProcurement systems** and it identified **44 interesting eProcurement Practices**. Based on a structured evaluation methodology (presented in Volume II), the contractor has deduced the eProcurement Practices and resulted in certain recommendations.

The identified eProcurement Practices are categorised into four groups, presenting innovative ideas and concepts for all aspects of an eProcurement programme. eProcurement Practices concerning **Organisational Aspects** are related to the organisation of an eProcurement programme. eProcurement Practices concerning **Procedural Aspects** refer to the procedures/workflows followed during the eProcurement lifecycle. eProcurement Practices concerning **Technical Aspects** are associated to solutions on technical implementation issues. eProcurement Practices concerning **Operational Aspects** can enhance the services offered to the public and private sector, through the adoption of operations that enforce compliance with the EU legislation.

The analysis of the background information has concluded that currently the eProcurement environment in Europe is very fragmented, due to the lack of common standards and a homogenous legal framework. Furthermore, most of the European eProcurement initiatives are based on existing commercial products that are not driven by EU directives. It is also apparent that different commercialisation policies of eProcurement platforms have been followed by MS. There exist significant delays in the development of eProcurement systems that model the evaluation process of Tender offers and the associated internal business processes of public administrations, as well as, handle security aspects related to user authentication and the utilisation of CPV codes.

Further analysis on the deduced eProcurement Practices was performed in order to determine the level of coverage of the main principles derived from the new EU public procurement legislation.

The next phase of the current project will further elaborate on the identified eProcurement Practices, generating functional requirements for conducting electronic public procurement under the EU framework and eLearning Demonstrators, aiming to help public administrations in their effort to deeply understand the new directives and to implement compliant eProcurement systems.

Abbreviations / Acronyms

Abbreviation or Acronym	Term
AGM	Agency of Government Management (Danish administration)
BCP	Business Continuity Plan
CA	Certification Authority
CPB	Central Purchasing Body
CPV	Common Procurement Vocabulary
DOC	Microsoft MS Word document (.doc)
DFPS	Department of Finance and Public Administration (Basque administration)
DPS	Dynamic Purchasing Systems
DRP	Disaster Recovery Plan
EC	European Commission
EU	European Union
FAQ	Frequently Asked Questions
GAS	Government Administration Services (Norwegian administration)
GUI	Graphical User Interface
HTTP / HTTPS	HyperText Transfer Protocol / Secure HyperText Transfer Protocol
IDA	Interchange of Data between Administrations
IT	Information Technology
MEAT	Most Economically Advantageous Tender
MINDEF	Ministry of Defence (French administration)
MoD	Ministry of Defence (Belgian administration)
MS	Member States
OGC	Office of Government Commerce (UK administration)
OJEU	Official Journal of the European Union
OSS	Open Source Software
PIN	Prior Information Notice
PDF	Portable Document Format
PQQ	Pre-Qualification Questionnaire
Q&A	Questions & Answers
RTF	Rich Text Format
SLA	Service Level Agreement
SME	Small-Medium Enterprises
SMS	Short Message Service
SSL	Secure Sockets Layer
UN/SPSC	Universal Standard Products and Services Code
VPN	Virtual Private Network
XLS	Microsoft MS Excel spreadsheet (.xls)
XML	eXtensible Markup Language

Glossary

Term	Description
Advanced Electronic Signature	Means an electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory (b) it is capable of identifying the signatory (c) it is created using means that the signatory can maintain under his sole control (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable
Authentication	Proving a user's identity. To be able to access a Website or resource, a user must provide authentication via a password or some combination of tokens, biometrics and passwords.
Authorisation	The act of granting approval. Authorisation to resources or information within an application can be based on simple or complex access control methods.
Basic Internet Security **Browser Based**	Typically employed in low value, low sensitivity applications using Secure Sockets Layer (SSL) for confidentiality, with the possible addition of UserID and Passwords for user authentication. This term describes software that does not require any client software to be installed or configured on users' systems, except of the commercially supported Web-browsers (IE, NS, Mozila and Opera). Unlike a browser plug-in, browser based applications do not require manual download and execution of an installation program prior to Web site access; Unlike an ActiveX control or some Java applets, browser based applications do not force the user to agree to potentially confusing security warning dialogs. Unlike other client applications, browser based applications do not have a noticeable download time. In fact, download is transparent to the end-user.
Certificate	An electronic "passport". A certificate is a secure electronic identity conforming to the X.509 standard. Certificates typically contain a user's name and public key. A CA authorises certificates by signing the contents using its CA signing private key.
Certificate validation	The process of checking the trustworthiness of a certificate. Certificate validation involves checking that the certificate has not been tampered with, has not expired, is not revoked and was issued by a CA you trust.
Certification Authority (CA)	The system responsible for issuing secure electronic identities to users in the form of certificates.
Cryptography	The science to convert plain language into coded text and in reverse.
Decrypt	To decrypt a protected file is to restore it to its original, unprotected state.
Electronic signature	Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication
Encryption	To encrypt a file is to apply a mathematical function that transforms character(s) in the file into some other character(s). Encryption renders the file unreadable. This means no one, including the actor, can read the file until it is decrypted. Only authorised recipients can decrypt the file.
Encryption key pair	This consists of the encryption public key and decryption private key. The public key portion of an encryption key pair is used to encrypt data which can be decrypted by the matching decryption private key.
Enhanced Internet Security **Identification**	This is the required level of security needed for applications that deal with higher value and higher sensitivity transactions and information. This consists of enhanced levels of identification, entitlements, verification, privacy and security management. see Authentication
National eProcurement Authorities	Refers to the public authority responsible for the eProcurement programme of a country, as well as, for compliant with the legislation operation of the offered systems. The information analysed in the current report has all been obtained by the National eProcurement Authorities of the participating countries.
Private key	The portion of a key pair that is kept secret by the owner of the key pair. Private keys sign or decrypt data.
Public key	The portion of a key pair that is available publicly.
Public Key	A system that provides the basis for establishing and maintaining a trustworthy

Infrastructure (PKI)	networking environment through the generation and distribution of keys and certificates. This is also the foundation technology for providing enhanced Internet security.
Secure Sockets Layer (SSL)	A secure session protocol used to maintain data confidentiality only between Web-browsers and Web servers. This is a fundamental component of basic Internet security.
Security Management	The act of effectively and efficiently managing identification, entitlements, verification and privacy such that there is less burden of administration for end users and administrators regardless of application or platform.
Security policy	An organisation's security policy governs the use of the appropriate infrastructure in the organisation to achieve security objectives.
Time Stamping	The validity of storing the official date and time a business transaction has occurred.
Web Portal	A Web portal is a single doorway for employees, customers and partners to access an organisation's content, data and services online. Also known as Enterprise portals, Web portals make it possible to establish online relationships by providing personalised content to different individuals and entities. Organisations are building portals not only to increase loyalty, but also to create competitive advantage, strengthen relationships, speed access to services and satisfy regulatory requirements. Portals also make it possible to increase revenue, efficiencies and cost savings by moving business processes online.
XML	XML is the standard messaging format for business communication, allowing companies to connect their business systems with those of customers and partners using the existing Internet infrastructure. Similar to HTML, XML uses tags (words bracketed by '<' and '>') and attributes (of the form name="value") to help place structured data into text files. XML is different from HTML in that it is a meta-language (a language for describing languages) and, therefore, does not define specific tags and attributes.

Table of Contents

Executive Summary 3
Abbreviations / Acronyms 4
Glossary 5
Table of Contents 7
Table of eProcurement Practices 9
1 Introduction 11
1.1 Structure of the report 11
2 Overview of the analysis methodology 12
3 Background Information 14
3.1 Creation of a homogeneous eProcurement environment across Europe 16
3.2 System requirements to be driven by the directives, rather than by the capabilities of existing commercial products 17
3.3 eProcurement systems supporting the bid evaluation process and other internal business processes of public administrations 17
3.4 Security aspects related with user authentication 18
3.5 Commercialisation policy for public eProcurement platforms/services 19
3.6 Utilisation of CPV codes 19
4 Procurement practices concerning organisational aspects 20
4.1 Approach for facilitating adoption of eProcurement programme 20
4.1.1 Helping public administrations to join an eProcurement programme 21
4.2 Contracting Authorities 21
4.2.1 Return-on-Investment (ROI) analysis for understanding the economic benefits generated by eProcurement 22
4.2.2 Change Management scheme for implementing eProcurement 23
4.3 Suppliers 23
4.3.1 Supplier adoption programme 24
4.4 Further analysis of eProcurement Practices related to organisational aspects 25
5 eProcurement practices concerning procedural aspects 26
5.1 Publishing Notices 26
5.1.1 Use of electronic messages to automate publication in the OJEU 27
5.1.2 Secure notification using email 28
5.1.3 SMS notification as an alerting mechanism 29
5.1.4 Matching supplier profile to business opportunities 30
5.2 Registration process 31
5.2.1 Offer multiple methods of registration 31
5.2.2 Obtain user profiles through the integration with back-office systems 32
5.3 Questions & Answers session 33
5.3.1 Moderate Questions & Answers session to ensure confidentiality 33
5.4 Short-listing of suppliers 34
5.4.1 Pre-qualification questionnaire for short-listing suppliers 34
5.5 Submission of Tenders 35
5.5.1 Mechanism for encrypting and locking submitted tenders 36
5.5.2 Updating a tender 37
5.5.3 Assist suppliers during tender submission through user-friendly GUI 37
5.5.4 Enable tendering through electronic forms 38
5.6 Tender opening 39
5.6.1 Phased opening of tenders according to the tender documentation type 40
5.6.2 Application of the Four-Eye Principle 41
5.7 eAuctions 42
5.7.1 Configure eAuction according to nature of procurement 43
5.7.2 Transform non-price criteria into monetary values 44
5.8 Offline activities 44
5.8.1 Tools for preparing tenders offline according to call specifications 44
5.8.2 eProcurement system to monitor offline activities by suppliers 45

5.9 Further analysis of eProcurement Practices related to procedural aspects 46
6 eProcurement Practices concerning technical aspects 48
6.1 Security 48
6.1.1 Utilisation of SSL to guarantee minimum communication security level 49
6.1.2 Secure communication between eProcurement and external systems 49
6.2 Electronic signatures 50
6.2.1 Limited use of electronic signatures (only for critical activities) 51
6.3 Time -stamping 51
6.4 Audit trailing 52
6.4.1 Matching logs from different modules and use a unified event log 53
6.4.2 Safe storage of system logs 54
6.5 Reporting 54
6.5.1 Generate reports on competitions using system event logs 55
6.5.2 Advanced statistical analysis on eProcurement data 56
6.6 Virus protection & protection from malicious attacks 57
6.6.1 Virus check tenders upon submission 57
6.7 Interoperability 58
6.7.1 Support multilingualism and parameterisation of the application 59
6.8 Integration Capabilities 59
6.8.1 Integration with financial systems 60
6.8.2 Establishment of a transactional hub to facilitate communication between different systems 61
6.9 Electronic document standards 62
6.9.1 Support of all widely used electronic document standards 62
6.10 Software adaptability 63
6.10.1 Workflow management for assisting the preparation of call documentation 64
6.10.2 Modelling procurement competition phases as a series of eProcurement events 65
6.11 Further analysis of eProcurement Practices related to technical aspects 65
7 eProcurement Practices concerning operational aspects 67
7.1 Operational support to participating organisations 67
7.1.1 Provide legal support to participating organisations 67
7.1.2 Organise training events simulating the real competition environment 68
7.1.3 Offer consultancy services to Contracting Authorities 69
7.2 Quality of content 70
7.2.1 Assure quality of supplier eCatalogues 70
7.3 Definition of Operational Requirements 71
7.3.1 Define level of services with the technology providers 71
7.4 Volume Capacity 72
7.4.1 Policy for extending eTendering deadline due to volume capacity problems 72
7.4.2 Implementation of a two -phased submission process 73
7.4.3 Allow the downloading of submitted tenders before eTendering deadline 74
7.5 Complaint Procedures 75
7.6 Further analysis of eProcurement Practices related to operational aspects 75
8 Conclusion 77

Table of eProcurement Practices

eProcurement Practice #1 Establishment of a transparent contracting relation plan 21
eProcurement Practice #2 Return-on-Investment (ROI) analysis for understanding the economic benefits generated by eProcurement 22
eProcurement Practice #3 Change Management scheme for implementing eProcurement 23
eProcurement Practice #4 Supplier adoption programme 24
eProcurement Practice #5 Use of electronic messages to automate publication to OJEU 27
eProcurement Practice #6 Secure notification using email 28
eProcurement Practice #7 SMS notification as an alerting mechanism 29
eProcurement Practice #8 Matching supplier profile to business opportunities 30
eProcurement Practice #9 Offer multiple methods of registration 31
eProcurement Practice #10 Obtain user profiles through the integration with back-office systems 32
eProcurement Practice #11 Moderate Questions & Answers session to ensure confidentiality 33
eProcurement Practice #12 Pre-qualification questionnaire for short-listing suppliers 34
eProcurement Practice #13 Mechanism for encrypting and locking submitted tenders 36
eProcurement Practice #14 Updating a tender 37
eProcurement Practice #15 Assist suppliers during submission through user-friendly GUI 38
eProcurement Practice #16 Enable tendering through electronic forms 39
eProcurement Practice #17 Phased opening of tenders according to the tender documentation type 40
eProcurement Practice #18 Application of the Four-Eye Principle 41
eProcurement Practice #19 Configure eAuction according to nature of procurement 43
eProcurement Practice #20 Transform non-price criteria into monetary values 44
eProcurement Practice #21 Tools for preparing tenders offline according to call specifications 45
eProcurement Practice #22 eProcurement system to monitor offline activities by suppliers 46
eProcurement Practice #23 Utilisation of SSL to guarantee minimum communication security level 49
eProcurement Practice #24 Secure communication between eProcurement and external systems 50
eProcurement Practice #25 Limited use of electronic signatures (only for critical activities) 51
eProcurement Practice #26 Matching logs from different modules and use a unified event log 53
eProcurement Practice #27 Safe storage of system logs 54
eProcurement Practice #28 Generate reports on competitions using system event logs 55
eProcurement Practice #29 Advanced statistical analysis on eProcurement data 56
eProcurement Practice #30 Virus check tenders upon submission 58
eProcurement Practice #31 Support multilingualism and parameterisation of the application 59
eProcurement Practice #32 Integration with financial systems 61
eProcurement Practice #33 Establishment of a transactional hub to facilitate communication between different systems 62
eProcurement Practice #34 Support of all widely used electronic document standards 63
eProcurement Practice #35 Workflow management for assisting the preparation of call documentation 64
eProcurement Practice #36 Modelling procurement competition phases as a series of eProcurement events 65
eProcurement Practice #37 Provide legal support to participating organisations 68
eProcurement Practice #38 Organise training events simulating the real competition environment 69
eProcurement Practice #39 Offer consultancy services to Contracting Authorities 70
eProcurement Practice #40 Assure quality of supplier eCatalogues 71
eProcurement Practice #41 Define level of services with the technology providers 72
eProcurement Practice #42 Policy for extending eTendering deadline due to volume capacity problems 73
eProcurement Practice #43 Implementation of a two-phased submission process 74
eProcurement Practice #44 Allow the downloading of submitted tenders before eTendering deadline 75

List of Tables

Table 1: Coverage of the EU legislation principles by the [*Name of the category*] eProcurement Practices 13
Table 2: Coverage of the EU legislation principles by the organisational eProcurement Practices 25
Table 3: Overview of the requirements for publishing notices 26
Table 4: Coverage of the EU legislation principles by the procedural eProcurement Practices 47
Table 5: Coverage of the EU legislation principles by the technical eProcurement Practices 66
Table 6: Coverage of the EU legislation principles by the operational eProcurement Practices 76
Table 7: Highly recommended eProcurement Practices 78

1 Introduction

The eEurope Action Plans 2002 and 2005 have set ambitious goals concerning the "Government online: electronic access to public services", requiring efforts by public administrations at all levels to exploit new technologies. The realisation of these goals would make information as accessible as possible and would improve services and interaction with citizens and businesses. One of the primary objectives of eEurope is to enable the use of electronic procurement (eProcurement) across Europe, creating common principles and technical suggestions for all MS. These principles and suggestions would facilitate an operational environment where public administrations could achieve better results through fairer and more effective competitions, while suppliers would be enabled to compete in an open and transparent framework, which ensures equal treatment and non-discrimination.

In late 2003, the Interchange of Data between Administrations (IDA) launched this specific project, whose purpose is twofold. The first objective is to establish functional requirements and produce guidelines for technical specifications:

- in compliance with the new EU public procurement legislative framework
- using input from a state of the art report on case studies on European electronic public procurement projects (current report)
- using input from analysis of electronic public procurement status and systems in non-European countries

The second objective of the project is to model the new procurement workflows, as described in the new EU legislation, and develop static and dynamic Demonstrators. The Demonstrators are to be made available to MS for educational and experimentation purposes, assisting in the definition of eProcurement system requirements and elaboration of functional requirements for systems that are fully compliant with the EU public procurement legislation.

1.1 Structure of the report

The current report is composed of two volumes. This document constitutes Volume I.

- **Volume I:** presents the conclusions of a state-of-the-art analysis as deduced from the reviewed MS countries and systems. eProcurement Practices are categorised in four groups:
  - ***Organisational*** practices for assisting administrations in establishing and developing eProcurement programmes
  - ***Procedural*** practices related to the phases of the eProcurement lifecycle for all foreseen procedures
  - ***Technical*** practices for modelling fully compliant with the legislation eProcurement systems from a technical viewpoint
  - ***Operational*** practices for establishing operations, assisting Contracting Authorities in conducting fair and transparent competitions
- **Volume II:** presents the background information through:
  - ***Methodology*** followed for the analysis
  - ***Countries*** that have been reviewed
  - ***Systems*** that have been analysed, categorised in Individual Contract, Repetitive Purchasing, eAuction, and secondary systems

2 Overview of the analysis methodology

eProcurement Practices constitute concepts, operational elements, technical implementations or any original ideas of MS, which can be considered as most useful features of an eProcurement programme or system. The deduced eProcurement Practices are grouped into four main categories, as detailed below:

- Organisational Aspects: eProcurement Practices for assisting administrations to conduct competitions, as well as, helping towards the development of eProcurement at national level
- Procedural Aspects: eProcurement Practices to be followed for all phases during the lifecycle of all foreseen eProcurement procedures
- Technical Aspects: eProcurement Practices for the technical modelling of eProcurement systems fully compliant with the new EU legislation
- Operational Aspects: eProcurement Practices for helping Contracting Authorities to conduct effective, fair and transparent competitions

The exact methodology used for the programme/system analysis, deduction/presentation of eProcurement Practices, and further analysis to highlight eProcurement Practices, is presented in the Methodology section of Volume II (section 2). Nevertheless, for completeness, the current chapter presents an overview of the methodology used.

Each eProcurement Practice is presented in the following way.

Description	*Brief description of the eProcurement Practice*
Functionality to be supported	*Functionality that has to be supported in order to establish the eProcurement Practice*
Implementation approach to follow	*Implementation steps that are necessary for the provision of the functionality*
System Module	*eProcurement module that provides the functionality (eNotification, eTendering, eAwarding, eInvoicing, ePayment)*
Principles satisfied	*(Equal Treatment, Transparency, Effectiveness, Interoperability, Security, General Availability, Confidentiality)*
Risks	*Principles that may be at risk by the implementation of the eProcurement Practice*
Input from	*Public administrations or eProcurement systems that provided input for the eProcurement Practice*

Number and Title of the eProcurement Practice

For the coverage of the legal requirements of the new European public procurement directives, compliance with the following principles has been examined:

- Tenderers receive an equal amount of information at the same time (equality of treatment)
- Contracting authorities respect the confidential nature of information (confidentiality)
- Mechanisms are supported, in order to record all system events and user activities, as well as, attempts to gain access to sensitive information (traceability)
- Operation of the system improves competition conditions for the users (effectiveness)
- Use of interoperable (compatibility) electronic means, generally available on the market or broadly used in MS, thus avoiding the use of country-specific or otherwise discriminatory technologies that restrict access to tendering procedures (interoperability).
- Use of technologies to ensure the secure communication of information and its storage in system data repositories (security)
- Use of technologies which are widely available and at low cost, as well as, mechanisms ensuring continuous operation of the system (general availability)

At the conclusions of the current report, all eProcurement Practices of a category are presented together in a form of a table, as demonstrated in Table 1.

No	[*Name of the category*] eProcurement Practices	Equal Treatment	Transparency	Effectiveness	Interoperability	Security	General availability	Confidentiality
1	*Title of the eProcurement Practice*			✓				
2	*Title of the eProcurement Practice*	✓		✓	?		✓	
3	*Title of the eProcurement Practice*			✓		✓		?
4	*Title of the eProcurement Practice*	✓	?	✓				

Table 1: Coverage of the EU legislation principles by the [*Name of the category*] eProcurement Practices

Separate symbols indicate which EU principles are satisfied by the eProcurement Practices (✓) and which are at risk (?).

3 Background Information

The report comprises two volumes. The current volume (Volume I) presents the results of the analysis, in terms of eProcurement Practices and conclusions, whereas Volume II provides all background information and detailed analysis of eProcurement status, legal framework, and state-of-the-art systems in the reviewed countries. The current section provides an overview of the reviewed countries and systems considered while the main conclusions of their analysis are also outlined.

The countries and public administrations examined in the context of the current analysis are presented in Figure 1.

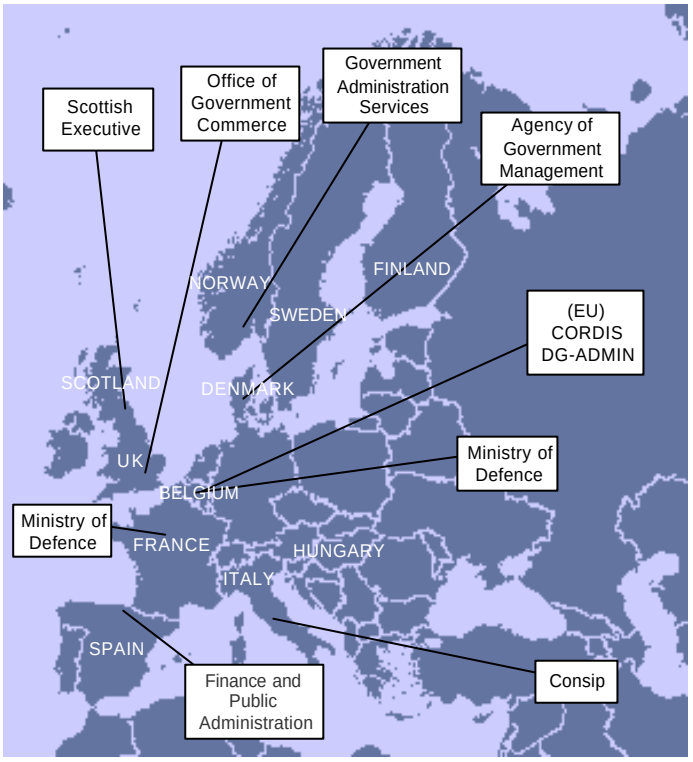

Figure 1: Reviewed administrations

The main purpose of the review was to identify the various approaches followed in each country for establishing eProcurement systems in the public sector. In this respect, the underlying development decisions and system implementations were considered. Furthermore, the functionality and technical features of the examined systems were analysed and their compliance with the provisions of the new public procurement directives was assessed. The results were presented in a systematic manner, according to the established evaluation methodology. Overall, 21 systems from 8 European countries were reviewed. The eProcurement procedure coverage of the systems is presented in Figure 2, whereas Figure 3 displays the eProcurement phases covered by the examined systems.

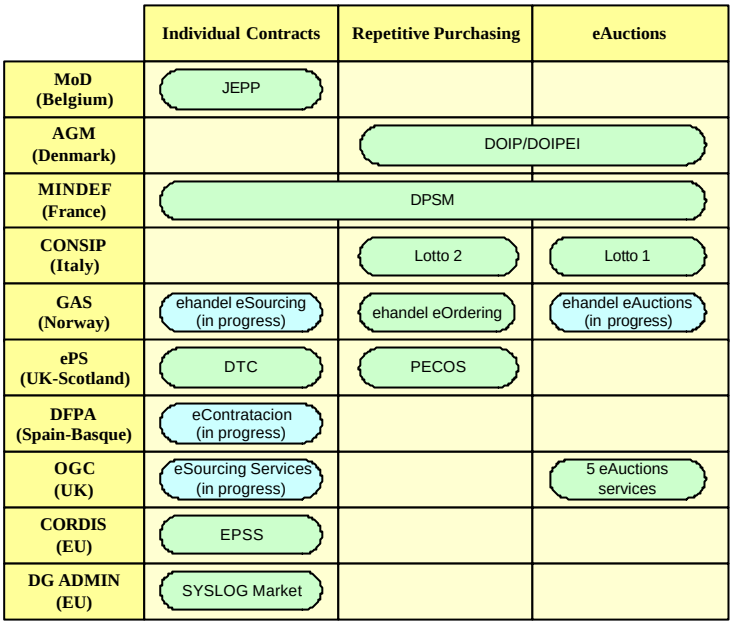

Figure 2: eProcurement procedures supported by reviewed systems

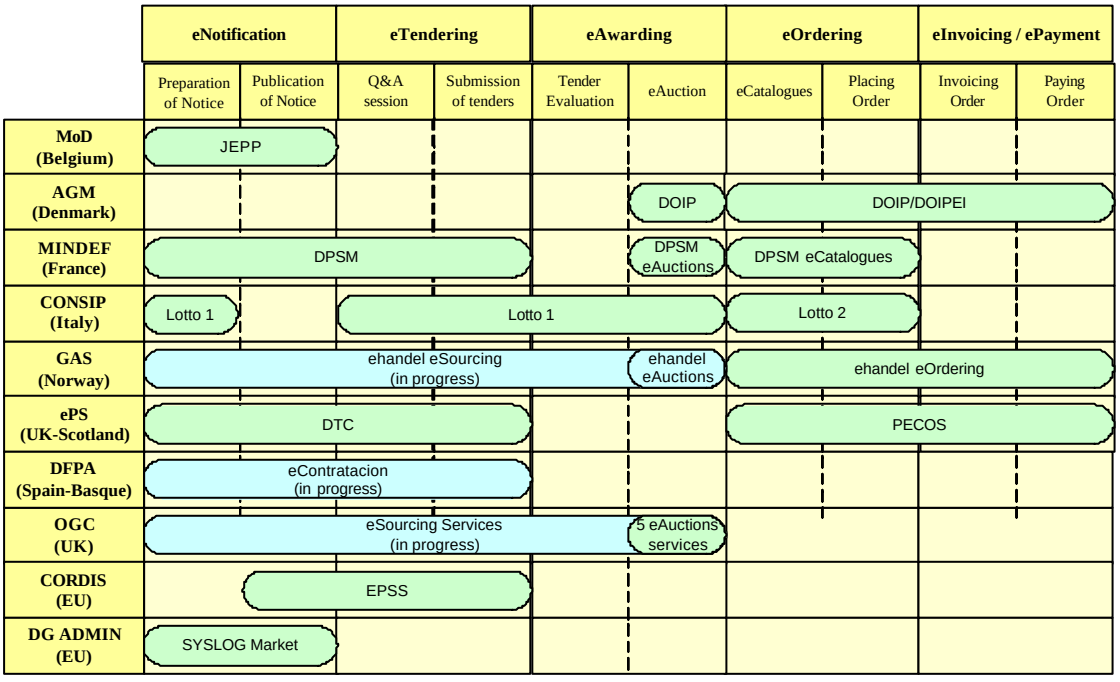

Figure 3: eProcurement phases supported by reviewed systems

The analysis of the reviewed countries and systems has resulted in some noteworthy conclusions with regards to existing trends in Europe.

3.1 Creation of a homogeneous eProcurement environment across Europe

All existing eProcurement systems throughout the reviewed countries have been conceived, designed, and implemented prior to the adoption of the new public procurement directives. Therefore, they are based on existing national legislative frameworks. As a result, none of the operational systems can fully support the necessary functionality required by the new directives.

Moreover, due to varying public procurement needs and national laws, priorities, and practices followed in the different countries, the various systems developed throughout the EU focus on the automation of different eProcurement procedures. Another inhomogeneous aspect in Europe is that of the terminology used. Currently, the lack of a unified terminology in the various reviewed countries can potentially cause misconceptions amongst EU institutions and/or economic operators that are involved with public eProcurement in Europe.

Some Member States have centralised eProcurement systems at government level (e.g. CONSIP in Italy). Other countries on the other hand, have decentralised public procurement, even if government is in charge of coordinating procurement. This means that there is not one single eProcurement system, but a number of different systems. In addition, the publication of notices is mostly electronic and is provided by several service providers and not the government.

The adoption of the new directives does not require the creation of a fully standardised eProcurement environment. Different approaches may co-exist. The aim is to facilitate the efficient introduction of eProcurement solutions in compliance with the new European public procurement regulatory framework. To achieve this, the IDA programme has established three objectives:

- to achieve a high degree of interoperability in electronic public procurement and assist efforts for developing concrete measures to overcome potential obstacles to the smooth functioning of electronic procurement across Europe
- to facilitate electronic public procurement by providing common functional requirements, common tools or generic services for the awarding entities and, as regards the suppliers, to enable easy access to public procurement opportunities in different Member States
- to promote the use of eProcurement in Europe by creating awareness of transborder eProcurement benefits and opportunities

The first step should constitute the establishment of a common understanding of all procedural requirements derived by the directives and their transposition to functional system requirements.

A second step should constitute the development of demonstrators simulating the eProcurement workflows. The demonstrators can be used for establishing a common and thorough understanding of eProcurement requirements between all actors involved in the public procurement lifecycle (procurement authorities, public administrations and suppliers). Their main purpose is to explain the underlying business logic of events (workflows and exceptions) described in the new directives, and thus to provide all actors with a facility to experiment, familiarise, and better understand the directives.

3.2 System requirements to be driven by the directives, rather than by the capabilities of existing commercial products

All systems examined in Member States are based on sophisticated eProcurement commercial marketplace products offered by vendors, with minimal customisations. Although this approach can initially facilitate the timely launching of eProcurement systems with relatively small investments, it results in public eProcurement systems that are software-driven rather than legislation-driven and demonstrate little flexibility. Therefore, expensive customisations are usually necessary for these systems in order to become compliant with the new EU directives.

3.3 eProcurement systems supporting the bid evaluation process and other internal business processes of public administrations

Among the existing systems reviewed in the current work, there is no functionality implemented for automating the evaluation of bids. As demonstrated in Figure 4, only 20% of the reviewed countries are currently attempting to establish a system that can facilitate the automated or semi-automated evaluation of tenders.

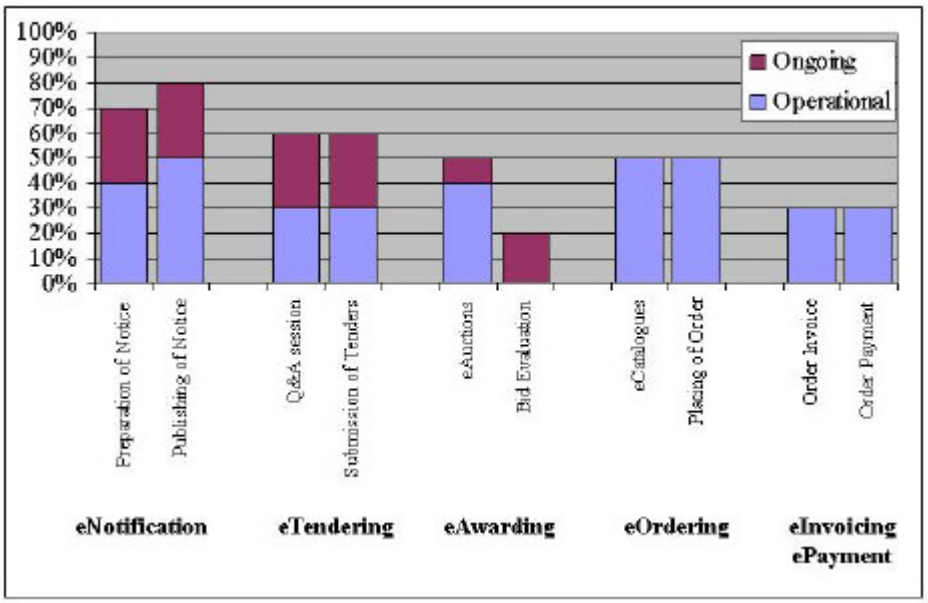

Figure 4: Coverage of the various eProcurement phases in the reviewed MS

This delay is due to the fact that eAwarding constitutes a complicated phase to model, as it depends on the details of each particular competition and involves the modelling and automation of business processes that are internal in a public administration. This requires customised solutions and integration with legacy systems that demand additional effort and expertise, while they are not usually supported by COTS systems.

Automation of bid evaluation is considered important, as it can drastically shorten the time for the completion of a call for tenders, whereas it greatly contributes to the transparency and full logging of the awarding procedure.

3.4 Security aspects related with user authentication

A crucial decision in all eProcurement implementations is related to the security policy employed. Depending on national legislation compliant with the eSignatures directive, there exist some implemented systems that require "soft" user authentication through user credentials (e.g. user names and passwords), while other systems support "hard" authentication through enforcing the use of advanced electronic signatures. Since the EU legislative framework does not specify a simple uniform solution for the use of any particular user authentication method, it is recommended for future systems to support a variety of authentication mechanisms, including user credentials, electronic signatures, and smart cards. This will significantly enhance the interoperability of eProcurement systems, whereas it will prohibit discrimination against foreign suppliers that cannot use certain PKI facilities, thus providing for generally available, easily accessible systems. Nevertheless there is a need to define minimum security requirements at a pan-European level. Each MS will then be able to implement solutions, satisfying local specific requirements abiding to minimum security requirements.

3.5 Commercialisation policy for public eProcurement platforms/services

The administrations in the reviewed countries follow different approaches in offering the established eProcurement services to Contracting Authorities and suppliers. Some of them have committed significant funds for the realisation and operation of their eProcurement initiatives, offering eProcurement services to all parties free of any charges. Their objective is to promote the further development and use of eProcurement systems in their countries, achieving a return-on-investment from the cost-savings achieved by public administrations. On the other hand, there are administrations that charge certain fees to Contracting Authorities, suppliers or both for using eProcurement services.

The former approach offers equal opportunities for participation to all parties; however benefits are difficult to measure. The latter approach on the other hand excludes suppliers/administrations that cannot afford the joining fee, possibly resulting in inequality of treatment.

The use of OSS software is expected to lower the overall cost of realising/operating eProcurement systems, and therefore lowering or even eliminating subscription/annual costs for suppliers and administrations.

3.6 Utilisation of CPV codes

EC Regulation 2195/2002 established Common Procurement Vocabulary (CPV) as the single classification system in public procurement. Most of the reviewed systems employ CPV codes, at the moment. A number of systems categorise products and services through United Nations Standard Products and Services Code (UN/SPSC), while other systems do not use at all a classification system. This is due either to that fact that such requirement does not appear in existing national legislations or to the fact that the associated functionality is not supported by the utilised COTS system. Irrespectively to the current use of a hierarchical classification system, the new EU public procurement legislation demands the usage of CPV codes in the publication of notices and statistical reporting, and therefore all existing systems should either utilise CPV codes, or be in position to map the codes from their classification system (i.e. UN/SPSC) to CPV codes.

4 Procurement practices concerning organisational aspects

This section reviews eProcurement Practices related to the organisational aspects of eProcurement and in particular focuses on how National eProcurement Authorities can assist public sector administrations to join eProcurement programmes, as well as, how to encourage suppliers to utilise eProcurement in order to conduct their business with the public sector.

A large number of eProcurement authorities contributed to the current report, providing information about eProcurement programmes, services, operational systems, and ongoing projects, in their country. The section is divided into three sub-sections looking at Procurement Practices involving the main actors: National eProcurement Authorities, Contracting Authorities, and Suppliers.

4.1 Approach for facilitating adoption of eProcurement programme

A National eProcurement Authority comprises an administrative body responsible for the introduction of eProcurement in its country. In some cases, these bodies are also responsible for implementing or supervising the operation of eProcurement systems in their countries.

Among the main activities undertaken by such authorities is the establishment of a national public eProcurement contracting framework which sets out the operation and the related hosting activities and services in the country. Also, the operation of eProcurement systems is a common activity. Typically, in such cases, the national eProcurement authority has a contracting framework with service/hosting providers, which defines the rules and regulations for service operation, including their SLA standards. In the countries examined, there have been identified two different types of arrangements:

- Three-party agreement: when a new Contracting Authority joins the service, a contract is created among the three parties (national authority – service provider – contracting authority), setting out the obligations and responsibilities for each party.
- Two-party agreement: when a new Contracting Authority joins the service, a contract is signed only between the service/hosting provider and the Contracting Authority, which has to abide to the rules and regulations of the "master contract", existing between the national eProcurement Authority and the service provider.

4.1.1 Helping public administrations to join an eProcurement programme

Irrespectively of the contracting set-up between the involved parties, it is considered very beneficial to have a transparent contracting relation plan. It has to be clear for a Contracting Authority what benefits and obligations will arise from such an agreement. The contract must clearly define the roles and responsibilities of each party, providing the necessary confidence to administrations joining the eProcurement programme. It is also important to provide means for reducing the time and effort a public administration needs to dedicate for joining an eProcurement programme.

Description	- Establishment of a transparent contracting relation plan - Assistance to public administrations for converting their traditional public procurement procedures to eProcurement
Functionality to be supported	N/A
Implementation approach to follow	- Define a clear contractual framework between all parties involved - Provide the necessary confidence to public administrations for using eProcurement by clearly defining roles and responsibilities - Reduce the time and effort a public administration needs to dedicate in order to join the eProcurement programme
System Module	N/A
Principles satisfied	Effectiveness
Risks	None
Input from	OGC (UK), ePS (UK/Scotland), Consip (Italy), GAS (Norway), AGM (Denmark)

Good Practice #1 Establishment of a transparent contracting relation plan

4.2 Contracting Authorities

There are numerous Contracting Authorities at different sizes and institutional character involved in the organisation of procurement competitions. They can be large government purchasing organisations (e.g. Ministries or central purchasing bodies), or small public organisations (e.g. municipalities).

A main obstacle that Contracting Authorities face is to understand the full potential of eProcurement and how it can be realised through the use of eProcurement solutions operating in the country. This obstacle becomes even more crucial when the exploitation model of the operating eProcurement systems requires the payment of subscription fees and training, or investment in IT equipment.

The following sections provide two identified eProcurement Practices related to organisational issues, which can help public authorities overcome the aforementioned difficulties.

4.2.1 Return-on-Investment (ROI) analysis for understanding the economic benefits generated by eProcurement

The majority of the reviewed EU administrations offer "pre-sales" or "return-on-investment" analysis, with forecasts on the economic benefits for a contracting authority from joining an eProcurement programme. Such analysis usually involves the study of historical data of the buying organisation, in order to deduce economic gains in terms of more effective competitions, more controlled repetitive spending, and time/effort gains due to the elimination of current bureaucratic procedures.

Description	- Provide a Return-on-Investment (ROI) study in order to help contracting authorities understand the economic benefits they can realise by joining an eProcurement programme - Assist contracting authorities in understanding their current spending procedures, and identifying potential causes of ineffectiveness - Help contracting authorities appreciate the effectiveness of competitions and repetitive purchases through eProcurement
Functionality to be supported	N/A
Implementation approach to follow	- Establish an "eProcurement adoption programme" which sets tangible goals for measuring the success of the program of contracting authorities joining the eProcurement programme - Conduct a Return-on-Investment (ROI) analysis for contracting authorities that are sceptical about joining the eProcurement programme - Consider the exact costs involved in rolling out the eProcurement system as the prime procurement mechanism for a contracting authority - Estimate necessary fees, IT investment, personnel training investment and any other set-up related costs - Educate public sector employees relating to eProcurement - Identify aspects of eProcurement that could achieve the most benefits and have the most tangible economic gains for the contracting authorities
System Module	N/A
Principles satisfied	Effectiveness
Risks	None
Input from	OGC (UK), ePS (UK/Scotland), Consip (Italy), AGM (Denmark), GAS (Norway)

Good Practice #2 Return-on-Investment (ROI) analysis for understanding the economic benefits generated by eProcurement

4.2.2 Change Management scheme for implementing eProcurement

In the process of assisting authorities to join an eProcurement service, National eProcurement Authorities usually analyse each joining organisation and identify the expected benefits. However such benefits can be achieved only if internal procedures of each buying organisation are altered in an appropriate way and the officers involved are educated in the use of electronic public procurement tools. Some National eProcurement Authorities have developed Change Management schemes, under which public sector organisations follow, in order to be advised as to how to achieve the most from eProcurement.

Description	- Develop a "Change Management" plan in order to help contracting authorities fully benefit from the adoption of eProcurement
Functionality to be supported	N/A
Implementation approach to follow	- Perform an analysis on the procurement procedures for each joining administration, in order to ascertain the areas that can generate the most benefits - Identify internal operations that can be modified in order to achieve the expected benefits - Perform statistical analysis of purchasing history and previous procurement competitions - Educate staff on the new EU legislation and the respective national legislative framework on eProcurement
System Module	N/A
Principles satisfied	Effectiveness
Risks	None
Input from	OGC (UK), ePS (UK/Scotland), Consip (Italy), AGM (Denmark), eContratacion (Spain/Basque)

Good Practice #3 Change Management scheme for implementing eProcurement

4.3 Suppliers

A significant consideration of contracting authorities is the participation of suppliers in the new type of electronic business. This is a crucial factor for the success of any eProcurement programme. All contracting authorities understand this fact and try to endorse the use of eProcurement in running fairer and more efficient competitions. However, this can only be achieved if suppliers also join the service and convert their business to eBusiness.

Attracting suppliers to an eProcurement service can be a significant obstacle, as this signifies changes to the way they conduct business with the public sector. This most probably involves significant costs. In particular SMEs that are often lacking funds or IT expertise, might consider eProcurement as a significant obstacle in conducting business with the public sector. This can result in exactly the opposite outcome from what EU wishes to achieve. Rather than creating an open-competition and equal-treatment-to-all environment, it can create a procurement environment where only certain types of suppliers participate in.

4.3.1 Supplier adoption programme

Norway, UK/Scotland and Spain/Basque have developed Supplier Adoption programmes, which are established in order to assist as many suppliers as possible participate in public procurement competitions. These programmes include a methodology under which suppliers are approached and educated in eProcurement, including analysis of their procedures, and recommendation of proposals as to the benefits they can achieve from eProcurement. Details on the Scottish approach to Supplier Adoption are presented in Volume II (section 4.4.1). Furthermore, most reviewed National eProcurement Authorities provide eProcurement services to suppliers at no cost, making their participation more appealing.

Description	- Educate suppliers (and in particular SMEs) in the benefits of eProcurement - Assist SMEs in modifying their internal procedures for benefiting the most from the adoption of eProcurement systems
Functionality to be supported	N/A
Implementation approach to follow	- Initial offer of the eProcurement services to suppliers at no cost - Charge suppliers only if they wish to use advanced integration capabilities with their legacy systems - Provide initial cost-free period to suppliers, until some benefits of joining the eProcurement programme can be realised
System Module	N/A
Principles satisfied	Equal treatment, Effectiveness
Risks	None
Input from	ePS (UK/Scotland), GAS (Norway), eContratacion (Spain/Basque)

Good Practice #4 Supplier adoption programme

4.4 Further analysis of eProcurement Practices related to organisational aspects

The section presents the results derived from the analysis of organisational eProcurement Practices. Table 2 demonstrates which principles are satisfied by the deduced organisational eProcurement Practices. As is immediately apparent, this category of eProcurement Practices is focusing on improving the effectiveness of eProcurement programmes. Well organised eProcurement programmes, modelling the aforementioned eProcurement Practices, can achieve tangible results, assisting all parties to appreciate the benefits they enjoy from eProcurement. Therefore, it is recommended that eProcurement National eProcurement Authorities consider the organisational aspects for improving the effectiveness of their programmes.

No	Organisational eProcurement Practices	Equal Treatment	Transparency	Effectiveness	Interoperability	Security	General availability	Confidentiality
1	Establishment of a transparent contracting relation plan			✓				
2	Return on investment analysis for understanding the economic benefits generated by eProcurement			✓				
3	Change management scheme for implementing eProcurement			✓				
4	Supplier adoption programme	✓		✓				

Table 2: Coverage of the EU legislation principles by the organisational eProcurement Practices

5 eProcurement practices concerning procedural aspects

This section presents the deduced eProcurement Practices from the review of various systems, modelling the different phases of the eProcurement lifecycle. Identified practices are grouped in eight categories modelled along the different phases of the procurement cycle. The categories for grouping eProcurement Practices related to procedural aspects comprise:

- **Publishing Notices:** Preparation and publication of notices to official electronic notice boards
- **Registration process:** Methods for creating user accounts and profiles with related roles
- **Questions & Answers session:** Online execution of Q&A sessions between Contracting Authorities and Economic Operators
- **Short-listing of suppliers:** Supplier qualification mechanisms based on the criteria that have been defined in the call for tenders notice
- **Submission of bids:** Mechanisms that enable the online preparation and submission of tenders
- **Bid opening:** Mechanisms for allowing the secure opening of tenders, following the simultaneous actions of two or more Procurement Officers
- **eAuctions:** Mechanisms for conducting electronic auctions
- **Offline activities:** Option for suppliers to perform certain activities outside of the system without being excluded from the competition or disadvantaged against other suppliers

Apart from the list of categories above, normally the procurement cycle also includes the Tender Evaluation, as well as, the Contract Awarding steps. Nevertheless, there are no identified practices for these two steps and therefore are not included in the subsequent sections.

5.1 Publishing Notices

The eNotification phase mainly consists of the publication of Preliminary Information Notices (PINs), Contract Notices (informing suppliers of new business opportunities), Corrigenda and Contract Award Notices (reporting the result of a competition). The publication notification requirements depend on the chosen awarding procedure. The following table presents the main requirements by type of competition and type of notice.

Awarding Procedure	Prior Information Notice	Contract Notice	Contract Award Notice
Individual Contracts			
Open	✓	✓	✓
Restricted	✓	✓	✓
Individual Contract within a			
Framework Agreement		✓	
Dynamic Purchasing System		✓	✓

Table 3: Overview of the requirements for publishing notices

5.1.1 Use of electronic messages to automate publication in the OJEU

The European legislation specifies contract value thresholds for public procurement above which the contract notices must be published in the Official Journal of the European Union (OJEU). It specifies the use of standard forms which are designed to comply with the legal requirements of the directives on the information Contracting Authorities should provide to Economic Operators. Automated publication in the OJEU can be achieved by the use of appropriately constructed XML files, complying with the SIMAP/TED XML Schema standard. This implies the need to develop an interface to OJEU. This eProcurement Practice is presented here.

Description	- Notices for calls for tenders above the EU contract value thresholds, to be automatically published on the OJEU
Functionality to be supported	- A contract notification must be submitted to the OJEU for official publication - On dispatch of the official publication to the OJEU, a system can publish the contract notifications onto its internal notification board, as well as, other official notification systems (national, regional, etc.)
Implementation approach to follow	- Implement mechanism for automatically sending notifications to the OJEU (i.e. above the EU threshold) - Establish interface with OJEU, by developing a tool that generates electronic messages according to the SIMAP/TED XML Schema (OJEU standard) - Use CPV codes in contract notices - Provide mechanism for becoming aware of the date/time a call for tenders was dispatched and published onto the OJEU - Develop interfaces with other notification systems (required by national laws) for automated simultaneous publishing
System Module	eNotification
Principles satisfied	Equal treatment, Transparency, Effectiveness
Risks	None
Input from	eSourcing Services (UK), DPSM (France), JEPP (Belgium), SYSLOG Market (EU), EPSS (EU), ehandel eSourcing (Norway)

Good Practice #5 Use of electronic messages to automate publication to OJEU

5.1.2 Secure notification using email

One of the prime objectives of the new EU legislative framework aims to create open eProcurement competitions. On this basis, the notification phase of an eProcurement competition is very important, as during this phase suppliers are made aware of new business opportunities. An effective notification mechanism is email, nevertheless it is widely known that the delivery of email messages is not guaranteed and from this respect email can lead to un-equal treatment.

To further enhance the use of email, the Scottish DTC system and the two Italian systems, are using a technique to ensure that the requirements of equal amount of information principle are preserved. The DTC and the Lotto systems have implemented a mechanism for creating a secure "inbox" for each supplier, which is hosted within the systems themselves. Therefore, the audit trailing mechanisms of the systems are capable of reporting at any time whether a supplier has read a particular notification (or any other email communication for this matter) and be aware of non-delivery problems if they exist.

Description	- Notification of suppliers for new business opportunities using email
Functionality to be supported	- Provide an email service for notifications to suppliers - Maintain a different email inbox for each supplier - Automatically notify suppliers based on their preferences
Implementation approach to follow	- Provide an email inbox for each supplier, in order to monitor whether a specific notifications has been read - Ensure that no user can obtain access to the email inbox of a supplier, in order to ensure confidentiality and equality of treatment
System Module	eNotification
Principles satisfied	Equal treatment, Transparency, Effectiveness
Risks	None
Input from	DTC (UK/Scotland), Lotto1 and 2 (Italy)

Good Practice #6 Secure notification using email

This functionality can also be used for all kinds of email notifications between contracting authorities and suppliers, and is not bound to new business opportunities notifications.

5.1.3 SMS notification as an alerting mechanism

Each Contracting Authority can define its own policy with regards to supplier notifications. Apart from the initial notification with a contract notice, a contracting authority may notify suppliers if and when there are modifications to the contract documents. It is considered important that a pre-defined policy is included in the details of the contract documents, precisely defining what online/offline steps will be taken by the Contracting Authority personnel in order to inform the supplier, without breaching the equal treatment principle of the EU legislation.

The use of Short Message Service (SMS) alerts offer an efficient solution for supplier notification, as planned to be implemented by the eSourcing Services in the UK. However, this mechanism, similarly to email, does not guarantee delivery and is considered as an untrustworthy communication method. Therefore, such notification method can be used only as supplementary to other notification mechanisms. Nevertheless, provided that other notification mechanisms are in place, SMS alerting can function as an instrument for further enhancing the automated alerting of suppliers.

Description	- Use Short Message Service (SMS) alerts as a supplementary notification mechanism
Functionality to be supported	- Enhance the email notification mechanism in order to overcome the issues of non-delivery of emails by utilising SMS alerts - Provide users with ability to set-up SMS alerting preferences (i.e. types of notifications to be sent, mobile numbers, delivery times, etc.)
Implementation approach to follow	- Establish a mechanism which notifies users even when they do not have access to email - Implement SMS messaging - Built-in to existing automated emailing notification system - Allow for SMS alerting preferences for each user
System Module	eNotification, eTendering
Principles satisfied	Equal treatment, Effectiveness
Risks	- SMS is not secure communication and therefore sensitive information may not be sent via this mechanism, in order to satisfy the confidentiality of information principle
Input from	eSourcing Services (UK)

Good Practice #7 SMS notification as an alerting mechanism

5.1.4 Matching supplier profile to business opportunities

Another eProcurement Practice on eNotification, employed by the Belgian and French systems, is the supplier profiling. The eProcurement application allows suppliers to set up profiles in their systems, specifying the types of business opportunities they are interested in. The system can search through published business opportunities and inform users of the ones they are most likely interested in. The supplier, when connected to the system, can visit his own Homepage and view these notifications. Furthermore, users can set-up an automated notification, such that they are informed of new business opportunities.

Description	- Utilisation of supplier profile to "push" information that might be of interest (new business opportunities)
Functionality to be supported	- Registered suppliers can define their profiles in terms of types of business and contracts they are interested in - Profiling can be flexible enough in order to allow suppliers to declare their preferences in several business sectors, as well as, specific types of business opportunities
Implementation approach to follow	- Apply a matching algorithm, capable of utilising all profiling information provided by suppliers and automatically identify all matching business opportunities - Store which business opportunities have been sent to which suppliers, in order to ensure that business opportunities are sent only once to a supplier - Use free text profiling fields, or more advanced standardised hierarchical coding schemes, like UN/SPSC or CPV
System Module	eNotification
Principles satisfied	Effectiveness
Risks	- The principle of equal treatment may be breached by this mechanism as certain suppliers will be better informed than others
Input from	JEPP (Belgium), DPSM (France)

Good Practice #8 Matching supplier profile to business opportunities

A potential Open Source application that can be utilised for the implementation of this eProcurement Practice is the Eureka search engine of the IDA Common Tools (Volume II – section 4.4.3).

5.2 Registration process

According to the EU legislation, Contracting Authorities may shorten the time-limits for receiving Tenders, when they offer unrestricted and full direct access by electronic means to the Contract Documents. The full tender documentation should be possible to be browsed and/or downloaded by suppliers with the minimum effort. There are no specific technical specifications on whether registration of suppliers prior to the downloading of documents needs to take place. Nevertheless, if a Contracting Authority requires a supplier to be registered before viewing/downloading the full tender documentation, the registration process may be as simple as possible. Apart from the registration process as such, registered users need to be given the appropriate access rights to the stored data, as well as, the actions they can perform on that data. This topic is usually referred to as "user profile".

The following two eProcurement Practices deal with these issues.

5.2.1 Offer multiple methods of registration

Some administrations may require the use of electronic signatures either for satisfying their national legal obligations for security, or for ensuring the best possible authentication when receiving tenders from suppliers. Furthermore, a number of offline activities may need to take place to confirm the identity of suppliers. In case a system requires the use of electronic certificates for user authentication, certain groups of tenderers, especially foreign suppliers, may be discriminated. As discussed in section 6.2, it is common for the use of advanced electronic signatures to be limited within the borders of the country of Certification Authority of a Member State. In order to ensure as open competitions as possible, multiple registration mechanisms may be made available, allowing the user registration and authentication irrespectively of the country of origin.

Description	- Provide multiple user registration processes
Functionality to be supported	- Allow users to choose preferred registration process - Simple registration process (requiring only trivial details) - Advanced registration process (use of electronic certificates)
Implementation approach to follow	- For simple registration process, allow for offline validation of supplier details - For systems utilising electronic signatures, an alternative simple registration process can be available for foreign suppliers
System Module	eTendering
Principles satisfied	General availability
Risks	- The registration details of suppliers need to remain secure in order to satisfy the confidentiality and equal treatment principles of the EU legislation
Input from	All systems

Good Practice #9 Offer multiple methods of registration

5.2.2 Obtain user profiles through the integration with back-office systems

A sophisticated eProcurement system, may involve the definition of many users from different departments of an organisation, along with user roles and workflows. The Danish DOIP/DOIPEI system has implemented an interesting approach to overcome the hurdle of multiple registrations for Contracting Authorities. Through the use of the BTS transaction hub (Volume II – section 4.2.3), the system allows for the integration with human resources or financial systems. Through this interface, the eProcurement system can easily obtain the details of all user profiles of the buyer that has subscribed to the eProcurement service. Participating public organisations need only to define and maintain user profiles in their back-office (HR or Financial) system and BTS ensures that the latest up-to-date user data is propagated and utilised in the eProcurement system.

Furthermore, this mechanism can also be regarded as a security feature of an eProcurement system. Such implementation ensures that if a user is not allowed to approve a purchase (above a certain threshold) in the financial system, the same will apply to the eProcurement system.

Description	- Integrate the eProcurement system to organisation's back-office systems in order to automatically obtain user profiles - Avoid duplication of effort in defining users and user profiles in more than one system - Ensure consistency of information across all systems
Functionality to be supported	- Integration with a back-office (HR or Financial) system for automatically obtaining all user related information - Hierarchical structures of the organisation automatically applied to the eProcurement system
Implementation approach to follow	- Create interfaces for automatically transferring user information from the back-office system(s) to the eProcurement system - Changes to user information are only performed in the back-office systems, and automatically replicated in the eProcurement system
System Module	All modules
Principles satisfied	Effectiveness, Interoperability
Risks	None
Input from	DOIP/DOIPEI (Denmark)

Good Practice #10 Obtain user profiles through the integration with back-office systems

5.3 Questions & Answers session

Following the notification phase, Contracting Authorities may operate a Questions and Answers (Q&A) session, also referred to as "Additional Documents". This provides the opportunity to suppliers to clarify all questions with regards to the tender documentation, as well as, the details of competition.

The Q&A area of the system must be open to all economic operators in an open competition, or all suppliers that have been qualified (in restricted and negotiated competitions). Furthermore, all participating suppliers should be in a position to post their questions to the Contracting Authority. To ensure equality of treatment, all participating suppliers need to have access to exactly the same clarifications.

5.3.1 Moderate Questions & Answers session to ensure confidentiality

The Scottish Executive identified that the way questions were sometimes formed by suppliers could disclose their identity, intended tenders or other sensitive information. For this purpose, the functionality of the Q&A in the Scottish DTC system is a moderated Frequently Asked Questions (FAQ) functionality. Suppliers can post their questions which are not made publicly available until approved by the Contracting Authority. Procurement officers can modify the suppliers' questions in an appropriate way before they are made public, in order to ensure confidentiality. Furthermore, the logging mechanisms of DTC ensures that all posted questions are recorded in the event history of the system and the Contracting Authority can report on the number of questions modified and/or not answered, in order to preserve confidentiality and transparency.

Description	- Implement moderated Q&A sessions ensuring confidentiality
Functionality to be supported	- The Q&A section of the system can support similar functionality to a typicalmoderated FAQ section - Allow participants to post their questions to a bulletin board
Implementation approach to follow	- Require approval by the bulletin board administrator before questions are made public - Answers to posted questions are possible to be provided only by the Contracting Authority, forbidding the direct dialogue between suppliers - The logging mechanisms of the system need to record all questions as submitted by suppliers, in order for the Contracting Authority to be in a position to report the number of questions that have been: o posted at any time o answered/unanswered o modified and for which purpose
System Module	eTendering
Principles satisfied	Equal treatment, Transparency, Effectiveness
Risks	- It is the contracting authority's responsibility to guarantee the confidentiality of information sent by suppliers
Input from	DTC (UK/Scotland)

Good Practice #11 Moderate Questions & Answers session to ensure confidentiality

The communication between Contracting Authority and suppliers can be restricted to the Q&A area of the system while no other communication (email, telephone, letter or otherwise) needs to be established between them. This requirement can ensure the equality of treatment between all suppliers, as the Q&A area is accessible by all and the same amount of information is presented to all suppliers.

5.4 Short-listing of suppliers

For the restricted procedure, the EU legislation foresees the short-listing or qualification of suppliers. The Contracting Authority can limit the number of candidates to take part in the competition according to pre-stated criteria. Initially, suppliers submit their expression of interest for a particular Call. Following the qualification procedure, the Contracting Authority short-lists the suppliers and invites a number of them to submit a Tender. In order to ensure a genuine/legitimate competition, the invited suppliers must be at least five for the restricted procedure and at least three for the negotiated procedure.

5.4.1 Pre-qualification questionnaire for short-listing suppliers

ePS has developed a Pre-Qualification Questionnaire (PQQ), a tool enabling the short-listing of suppliers for restricted competitions. PQQ is a questionnaire requesting preliminary information by suppliers, and is developed in such way that it can be used for different types of purchases. The functionality of DTC allows for the PQQ to be modelled as an Electronic Web Form, which however is not currently operational

The evaluation of PQQs and the short-listing of suppliers is probably the simplest evaluation procedure the Contracting Authority needs to perform. The evaluation function required for PQQs is usually a simplified check-list of a number of fields using Electronic Forms.

Description	- Short-list suppliers based on the answers provided to a pre-qualification questionnaire published with the contract notice
Functionality to be supported	- A PQQ module can be modelled as an electronic form, configurable to accommodate different competitions
Implementation approach to follow	- Construct electronic forms which implement the PQQ, allowing for its automated evaluation - Evaluation criteria can be configurable according to the type and complexity of the contract - An automated notification tool can inform all suppliers of their qualification status and exclude the disqualified suppliers from all future communications - The audit trailing mechanism needs to be in a position to record all activities (and justifications) for the qualification/disqualification of suppliers
System Module	eTendering
Principles satisfied	Equal treatment, Transparency, Effectiveness
Risks	None
Input from	DTC (UK/Scotland)

Good Practice #12 Pre-qualification questionnaire for short-listing suppliers

5.5 Submission of Tenders

The eTendering phase primarily consists of the electronic submission of tenders. In the restricted and negotiated procedures, a preliminary selection stage is involved, when only qualified suppliers are invited to submit a tender.

The eTendering phase of eProcurement is complicated as various aspects of the legislation need to be considered for a fully compliant system. Apart from the workflow of events during submission, consideration needs to be given to several technical aspects, for instance security and authenticity, as well as, operational matters, for instance the procedures following a system failure.

The system needs to be in a position to identify and authenticate a supplier during the submission process. The authentication of suppliers is a very sensitive area, as MS need to find a balance between two slightly contrasting issues; interoperability and security. The first principle implies the creation of an operational environment where all suppliers can participate to competitions using interoperable tools, satisfying minimum requirements. The second principle implies the possibility to verify suppliers' identity in an electronically secure way.

A crucial functionality for an eProcurement system is its ability to "lock" all submitted tenders until the pre-defined Tender opening time and/or until designated procurement officers authorise the opening of Tenders following simultaneous action. Tender protection is discussed further below.

A Contracting Authority can define its policy with regards to corrupted and virus infected tender files. The eProcurement system of a Contracting Authority, when receiving a tender, may automatically perform validity checks in order to ensure that the tender is not corrupted or virus-infected. Nevertheless, the policy may instead necessitate the suppliers to perform such validation checks. Checking for the validity of bidding document is discussed in more detail in section 6.6.

Four eProcurement Practices have been identified in the tender submission phase.

5.5.1 Mechanism for encrypting and locking submitted tenders

The French DPSM system has developed a mechanism for securing the transmission and storage of supplier tenders. Through this mechanism, when a supplier uploads a tender to the eProcurement system, a virus check is performed first. Assuming no detection of a virus, the document is encrypted according to a private key which is created for each competition. Subsequently, the tender documents are stored in a secure hosting environment, until their opening time. Only the president of the contract awarding committee can obtain the private key for decrypting the tender documents, which in turn can be obtained from the system only after the expiration of the eTendering deadline, as described below.

Description	- Provide a mechanism for ensuring that uploaded tenders are stored in a secure environment and remain inaccessible until the pre-specified bid opening time
Functionality to be supported	- Encrypt tender before submission - Submitted tenders remain locked by the system until the designated tender opening time - Decryption keys are used for tender opening
Implementation approach to follow	- Force the encryption of tender before submission - Provide a "tender locking" mechanism that ensures nobody can access the tender documentation - Every attempt to gain access to locked tenders is recorded to the system's logs - Decryption keys are disseminated to authorised personnel only after the eTendering deadline is reached
System Module	eTendering
Principles satisfied	Equal treatment, Transparency, Security, Confidentiality
Risks	None
Input from	DPSM (France)

Good Practice #13 Mechanism for encrypting and locking submitted tenders

5.5.2 Updating a tender

Further to the submission of tenders, and assuming the deadline for tender submission has not expired, a supplier can be provided with the functionality to update his submitted tender documentation. A version control mechanism may be used in this area, so that previous versions of documents are not completely discarded from the system, as this may be in use in cases of disputes or reporting purposes by the Contracting Authority.

Description	- Provide a mechanism for allowing suppliers to update their tenders before the expiration of the eTendering phase
Functionality to be supported	- Suppliers can update their submitted tenders as long as the eTendering phase has not expired
Implementation approach to follow	- A version control tool can be utilised to monitor the date and time of tender updates, previous versions, and history of tender modifications - Only the latest version of the tender may be regarded as valid - All previous tender versions cannot be opened unless in case of disputes
System Module	eTendering
Principles satisfied	Effectiveness
Risks	None
Input from	DTC (UK/Scotland), DPSM (France), eSourcing Services (UK)

Good Practice #14 Updating a tender

5.5.3 Assist suppliers during tender submission through user-friendly GUI

Sometimes tenderers find the eTendering process incomprehensive, especially when complicated procedures (for example electronic signatures) are involved. Furthermore, eProcurement system implementers need to always have in mind that tenderers do not use such eProcurement systems on an everyday basis. Therefore, suppliers and especially SMEs with limited IT experience are not necessarily familiarised with the complete functionality of the available system.

To tackle this issue, the MINDEF of France implemented an easy-to-use interface in order to assist tenderers to complete all steps during the eTendering process. When users want to upload a tender, they are presented with a popup window, where on the left hand side they can see the whole path of the eTendering process (the so-called "metro-line") and on the right hand side messages from the system. Colour coding is used in order to assist users in the whole submission process, immediately highlighting the completed (blue colour), pending (green colour) and failed (red) steps of the procedure. Furthermore, animations are used to keep the users informed of the progress of time-consuming actions, such as uploading large documents. "Metro-line" is particularly helpful for suppliers which do not intend to complete the whole submission process at once, serving as a reminder for all pending steps before completion.

Description	- Use GUIs that guide suppliers during the tender submission phase - A badly designed GUI can result in users not feeling in control of the situation, especially when long response times are involved - Avoid users abruptly stopping the eTendering process or being unsure as to whether certain tasks have been completed successfully
Functionality to be supported	- A user-friendly GUI can assist users to understand the eTendering process - Always inform users as to their pending tasks and corresponding deadlines
Implementation approach to follow	- Inform suppliers through the GUI of the complete procedure to follow - Use colour coding, animations and other visual effects to significantly improve the user-friendliness of the system
System Module	eTendering
Principles satisfied	Equal treatment, Effectiveness, Interoperability
Risks	None
Input from	DPSM (France)

Good Practice #15 Assist suppliers during submission through user-friendly GUI

5.5.4 Enable tendering through electronic forms

The legislation requires that the tools to be used for communicating by electronic means, as well as, their technical characteristics, must be non-discriminatory, generally available, and interoperable with the information and technology products in general use. Subject to satisfying these conditions, a Contracting Authority may specify the type (and version) of applications that can be used in order to generate and submit the tender documentation, as well as, provide templates to suppliers assisting them in providing all necessary information.

As modelled in all reviewed eAuction systems, the tender can be placed through electronic forms. Through this mechanism, the Contracting Authority can clearly define the information required by suppliers, as well as, ensure that all received tenders conform to the call for tenders specifications. Another benefit of electronic forms is that they allow for the automated evaluation of bids.

Description	- Provide electronic forms for the submission of tenders by suppliers - Allows for the automatic processing and evaluation of tenders
Functionality to be supported	- Use of electronic forms for the online preparation and submission of tenders
Implementation approach to follow	- Allow for the creation of electronic forms containing all necessary information to be completed for the submission of tenders - Including supplier help tools for completing the forms - Employ tender validation techniques, which can ensure tenders are compliant with call for tenders specifications - Offered mechanism need to be flexible enough to create a wide range of forms, in terms of layout, validation functions, multilingualism and localisation
System Module	eTendering
Principles satisfied	Equal treatment, Effectiveness
Risks	None
Input from	All eAuctions systems

Good Practice #16 Enable tendering through electronic forms

5.6 Tender opening

The opening of bids is a sensitive phase of the eProcurement procedure, as during this process the Contracting Authority gains access for the first time to the full tender documentation from all tenderers. The European legislation defines that the access to data transmitted electronically by tenderers can be possible only through simultaneous action of different authorised persons.

The Contracting Authority can have a dedicated space for each tender, where the submitted tenders are stored until the opening phase. A crucial procedure that needs to be followed during tender opening is to analyse the system logs and identify any attempts for accessing the tender documents during the locking period, as well as, if these attempts have been successful. If such an incident is captured, the Contracting Authority may have plans in place for handling the situation. Under no circumstances though, there can be any compromise to the required transparency standards that need to be achieved.

The following two eProcurement Practices are related to the process of opening tenders.

5.6.1 Phased opening of tenders according to the tender documentation type

According to the legislation of some MS, the tender documentation submitted by suppliers may be comprised by several distinct parts (e.g. proof documents, financial and technical offers). So, for example, the technical documentation of all tenderers should be opened and evaluated first, before their financial offer is opened. The following eProcurement Practice support this "phased opening approach" of opening tenders. Currently, this approach is supported by the French DPSM system.

Description	- Allow the opening of tenders in different phases - Each phase considers a different type of the tender documentation (proof documents, technical offer, financial offer, etc.)
Functionality to be supported	- Request supplier to complete and submit all pre-specified types of tender documentation - Proceed to the opening process in phases - Simultaneous unlocking of all tender documentation of the same type in each phase (i.e. all technical offers first, followed by all financial offers, etc.)
Implementation approach to follow	- Define types of documents that have to be included in each tender documentation package - Produce different decryption keys for each type of document - Unlock one type of tender documents in each phase
System Module	eAwarding
Principles satisfied	Equal treatment, Transparency, Effectiveness, Security, Confidentiality
Risks	None
Input from	DPSM (French)

***Good Practice #17** Phased opening of tenders according to the tender documentation type*

5.6.2 Application of the Four-Eye Principle

Another requirement of the EU legislation is the Four-Eye Principle, which states that at least two authorised procurement officers of the Contracting Authority can initiate the tender opening, by their simultaneous action. This is again an effort to enhance the transparency of such systems. The legislation does not define the exact specifications for the simultaneous opening of tenders by authorised persons. Many different technical solutions exist. Currently, the Basque eContratacion system is the only EU system which fully supports this aspect of the legislation. When a tender is submitted, the system fragments all tender files in segments, and these segments are owned by the various procurement officers. On opening time, each procurement office needs to contribute their file segments, before an assembler joins all segments to regenerate the initial tender. Furthermore, the individual file segments are encrypted on submission, so the procurement officers can not gain access to their portion of the tender, before the tender opening time.

Description	- According to the Four-Eye Principle, at least two appointed procurement officials are required to simultaneously authorise the opening of tenders
Functionality to be supported	- Designate two or more procurement officers to authorise the opening of tenders - Ensure tenders are inaccessible, unless the authorised procurement officers approve their unlocking
Implementation approach to follow	- In a software solution, two or more users of the Contracting Authority would be required to enter their passwords simultaneously (within a preset timeframe), before the unlocking of tenders is performed - Another software solution is the automated fragmentation of tender files on submission, each fragment being owned by a procurement officer. Only at opening time can procurement officer re-assemble the initial tender by all submitting their portion of the tender. Furthermore, file fragments are encrypted and can only be decrypted at opening time - An alteration of the above solution is to encrypt a tender during submission, and fragment the decrypting key. - In a hardware solution, two or more users of the Contracting Authority would be required to utilise smart cards (with electronic signature), followed by the provision of a password, in order to authorise the opening of the tenders
System Module	eAwarding
Principles satisfied	Transparency, Confidentiality
Risks	None
Input from	eContratacion (Spain/Basque)

Good Practice #18 Application of the Four-Eye Principle

5.7 eAuctions

The new EU legislation allows for the use of auctions. The Contracting Authorities may decide that the award of a public contract shall be preceded by an electronic auction provided the contract specifications can be established with precision. This allows Contracting Authorities to achieve better offers by suppliers before awarding the contract, while allows suppliers to improve aspects of their tenders. Tenders from all qualified suppliers are already evaluated at this stage, so the purpose of eAuction is to seek for better prices, quality, quantity or other quantifiable aspects of the suppliers' tenders.

eAuctions can be organised for the open, restricted and negotiated procedures, as well as, for the re-opening of competitions for framework agreement and DPS competitions. The use of eAuction should be stated in the Contract Notice. The specifications for the contract must detail:

- the features, the values for which will be the subject of electronic auction, provided that such features are quantifiable and can be expressed in figures or percentages;
- any limits on the values which may be submitted, as defined in the specifications relating to the subject of the contract;
- the information which will be made available to tenderers in the course of the electronic auction and, where appropriate, when it will be made available to them;
- the relevant information concerning the electronic auction process;
- the conditions under which the tenderers will be able to bid and, in particular, the minimum differences which will, where appropriate, be required when bidding;
- the relevant information concerning the electronic equipment used and the arrangements and technical specifications for connection.

On submission of a bid, the Contracting Authority needs to be in a position to instantly evaluate the offering. Therefore, a pre-requisite for effective eAuctions is the immediate parsing and processing of a bid, and the ranking of all bids on best offer sorting. Furthermore, the Contracting Authority must define the features/values which will be the subject to the eAuction. All reviewed eAuction systems use electronic forms (i.e. Web forms). This approach, apart from instant evaluation of bids, allows Contracting Authorities to clearly define the biddable fields, and the validation rules, ensuring that only valid bids, which conform to the call for tenders specifications, are accepted.

The definition of evaluation formulas requires significant amount of analysis and experience. An evaluation formula that contains many parameters can offer the possibility for suppliers to improve their offerings in many areas of their bid. Nevertheless, such formulas require a considerable amount of fine-tuning; otherwise they can be easily exploited. Both Contracting Authorities and suppliers may have to fully understand this formula before the eAuction takes place. In this respect, the OGC offers specialised consultancy services for the analysis of the Contracting Authority's needs and the construction of a robust evaluation formula. This is an eProcurement Practice from the OGC, otherwise buyers may either dedicate significant time to train their staff, or run the risk of being bound to the result of an eAuction in which it is not guaranteed that the best possible offer was achieved. Such aspects are discussed in section 7.1.

The following two eProcurement Practices are related to the eAuctions phase.

5.7.1 Configure eAuction according to nature of procurement

The definition of an eAuction can be flexible enough to accept various rules, depending on the goods/services being procured. Therefore, parameterised methods for setting up an eAuction are necessary. The OGC approach of supplying 5 different eAuction services, providing different functionality is an approach for such flexibility. Moreover, all reviewed eAuction systems are highly parameterised, where during the definition of the event the user can configure the type of eAuction competition. The following eProcurement Practice is proposing a way an eAuction can be configured.

Description	- Configure different eAuction events depending on the nature of procurement
Functionality to be supported	- Configurable aspects of an eAuction can cover the following areas: o Electronic forms for bidding o Number of rounds (if applicable) o Rules for deadline extension (if applicable) o Ranking information provided to suppliers o Call for tenders specifications ▪ Minimum and maximum decrements for the total economic offer ▪ Minimum and maximum values for each bidding field of the electronic forms
Implementation approach to follow	- Support several variations of the classic reverse auction events - Parameterisation according to type of business opportunity (i.e. types of goods/services procured, number of participating suppliers, etc.) - Parameterisation according to objectives set by the Contracting Authority (i.e. achieve better price, better quality, increased quantity, etc.) - Allow for the configuration of o Confidentiality rules to be applied (visibility of bid details) o Mandatory bidding fields o Mathematical formula for automatic evaluation of bids o Deadline extension pre-requisites o Communication methods with suppliers during bidding phase
System Module	eAwarding
Principles satisfied	Effectiveness
Risks	None
Input from	5 eAuctions services (UK), Lotto 1 (Italy), DOIP eAuctions (Denmark), ehandel eAuctions (Norway)

Good Practice #19 Configure eAuction according to nature of procurement

5.7.2 Transform non-price criteria into monetary values

The French system uses a simplistic mechanism for achieving the Most Economically Advantageous Offer in eAuctions with a single criterion (price). All non-price criteria are transformed into monetary values through pre-defined rules. This value, the so-called "handicap", is deducted from the tenderers' tender price, depending on the conformity of the tenderer's offer to the pre-specified criteria. Therefore, all criteria of the eAuction are reflected into a change in the bid price. The "handicap" mechanism is applied only to the initial tender, as after the eAuction starts suppliers can only bid on price. The following eProcurement Practice is describing this mechanism.

Description	- Provide a mechanism for transforming non-price related criteria of an eAuction bid into monetary values
Functionality to be supported	- Conduct eAuctions with price as the only criterion - Transform all other criteria into monetary values and apply them onto the initial tender price of the supplier
Implementation approach to follow	- Assign a monetary value for non-price criteria possible values (handicaps) - Automatic application of handicaps on supplier's initial tender price
System Module	eAwarding
Principles satisfied	Effectiveness, Transparency
Risks	None
Input from	DPSM (France)

Good Practice #20 Transform non-price criteria into monetary values

5.8 Offline activities

5.8.1 Tools for preparing tenders offline according to call specifications

An eProcurement Practice, employed by the EPSS system of the European Commission, is the ability to use an offline application for preparing tender documentation. The application allows for the preparation of the Part A and Part B of a typical CORDIS-FP6 proposal through electronic forms. Part A constitutes high-level information about the proposal and is broken down to three sub-sections: A1 containing general information about the proposal (i.e. title, description, call ID, activity code, etc.), A2 containing the company and contact details of each participating partner (i.e. company name, address, legal status, department involved, etc), while A3 constituting the financial offer (prices per partner). Furthermore, the offline tool also allows for the attachment of documents in Part B. Finally, the tool can compact all completed parts of the proposal into a package, which in turn can be uploaded onto the main EPSS online system. This mechanism provides an automated validation process for the proposals.

Description	- Offer suppliers with the possibility to prepare tender documentation offline - Guarantee the compliance of tender documentation with call for tenders specifications
Functionality to be supported	- Provide a tool which allows the offline preparation of tender documentation - Use pre-defined templates, exploiting the benefits of electronic forms (user help, validation rules, etc.) - Export all details in printer-friendly documents - Upload tender package completed offline onto the main system
Implementation approach to follow	- Support the partial preparation of tenders, by allowing suppliers to save and continue preparing their tenders in stages - Allow for the definition of customisable forms (depending on the buyer's requirements) - Employ flexible data validation rules - Provided tool to be portable to as many operating systems as possible - Encryption of tender documentation can be achieved by the offline tool
System Module	eTendering
Principles satisfied	General availability
Risks	- Tenders prepared offline may abide to the same rules as an online submission tool, to ensure confidentiality and equal treatment.
Input from	EPSS (EU)

Good Practice #21 Tools for preparing tenders offline according to call specifications

5.8.2 eProcurement system to monitor offline activities by suppliers

Suppliers may be given the opportunity to submit their partial or full set of documentation in a non-electronic format. Therefore, the system could be modelled in such a way, so that the details of communications using traditional paper-based means can be traced and linked to the eProcurement system. The Scottish DTC system has implemented a mechanism for allowing the storage and tracking of offline activities. Scottish Executive allows suppliers to contact the Contracting Authorities through telephone or FAX and furthermore submit their full or partial documentation of any eProcurement activity through the post. When such offline activity occurs, procurement officers can log into the DTC and update the system with the contact details, which are then stored automatically in the audit trailing (logs) mechanism of the system. The following eProcurement Practice refers to this approach.

Description	- Allow suppliers to perform eProcurement activities offline
Functionality to be supported	- Allow procurement officers to input information in the eProcurement system obtained through offline activities of suppliers
Implementation approach to follow	- Procurement officers can be given the option to connect to the system and perform certain activities on behalf of a supplier who has carried out an activity offline (i.e. post questions) - The audit trailing mechanism of the system should record that a procurement officer is performing actions on behalf of a supplier, including details of each action - Generate reports, detailing the exact activities performed by procurement officers, and sent to suppliers, for review and validation - Ensure the confidentiality of all tenders submitted offline (documents stored in a safe area and remain sealed until the tenders' opening time)
System Module	eTendering
Principles satisfied	Equal treatment, General availability
Risks	- When procurement officers perform activities on behalf of suppliers, transparency (i.e. list of activities performed) and confidentiality (i.e. denial of access to sensitive information) need to be ensured.
Input from	DTC (UK/Scotland)

Good Practice #22 eProcurement system to monitor offline activities by suppliers

5.9 Further analysis of eProcurement Practices related to procedural aspects

This section summarises the results derived from the analysis of the most useful eProcurement Practices related to procedural aspects. Table 4 lists the main principles satisfied by the eProcurement Practices, and the associated potential risks. This group of eProcurement Practices focus on the improvement of the effectiveness of eProcurement system.

No	Procedural eProcurement Practices	Equal Treatment	Transparency	Effectiveness	Interoperability	Security	General availability	Confidentiality
5	Use of electronic messages to automate publication in the OJEU	✓	✓	✓				
6	Secure notification using email	✓	✓	✓				
7	SMS notification as an alerting mechanism	✓		✓				?
8	Matching supplier profile to business opportunities	?		✓				
9	Offer multiple methods of registration	?					✓	?
10	Obtain user profiles through the integration with back-office systems			✓	✓			
11	Moderate Questions & Answers session to ensure confidentiality	✓	✓	✓				?
12	Pre-qualification questionnaire for short-listing suppliers	✓	✓	✓				
13	Mechanism for encrypting and locking submitted tenders	✓	✓			✓		✓
14	Updating a tender			✓				
15	Assist suppliers during submission through user-friendly GUI	✓		✓	✓			
16	Enable tenderingthrough electronic forms	✓		✓				
17	Phased opening of tenders according to the tender documentation type	✓	✓	✓		✓		✓
18	Application of the Four-Eye Principle		✓					✓
19	Configure eAuction according to nature of procurement			✓				
20	Transform non-price criteria into monetary values		✓	✓				
21	Tools for preparing tenders offline according to call specifications	?					✓	?
22	eProcurement system to monitor offline activities by suppliers	✓	?				✓	?

Table 4: Coverage of the EU legislation principles by the procedural eProcurement Practices

6 eProcurement Practices concerning technical aspects

This section presents all deduced eProcurement Practices that relate to the technical implementation of the various eProcurement modules. The objective is to present all state-of-the-art concepts, which offer technical solutions to common issues of modelling an electronic procurement system. Eleven categories have been identified for grouping eProcurement Practices related to technical aspects:

- **Security:** Issues related to the safe transmission, storage and utilisation of data
- **Electronic signatures:** Issues related to the implementation approach of strong authentication methods and the particularities of electronic signatures
- **Time-stamping:** Mechanisms for ensuring accurate timing of system events
- **Audit trailing:** Methods for keeping a history of performed system activities and capability of reconstructing past events
- **Reporting:** Mechanisms for obligatory reporting and decision making purposes
- **Virus protection & protection from malicious attacks:** Issues related to deliberate or unintended attacks on the system and ways to provide protection
- **Confidentiality:** Mechanisms for ensuring that all imported and generated data are safe and confidential
- **Interoperability:** Implementation approaches for achieving interoperability of the system to various platforms and utilisation of pan-European standards
- **Integration capabilities:** Mechanisms for creating interfaces between the eProcurement system and external (buyer or supplier) systems
- **Electronic document standards:** Adoption of specific standards related to documents and data exchange
- **Software adaptability:** Software development methods for ensuring the longevity of the system

6.1 Security

During the development of eProcurement systems, there is a variety of security issues that need to be considered: for instance the secure transmission, safe storage, consistency and confidentiality of data. A very sensitive area of security is the methods employed for authenticating users in the system, as information exchanged between Contracting Authorities and suppliers is commonly binding.

A lot of eProcurement solutions have faced a number of problems arising from the implementation of strong rules of security. Strong security measures may make the system difficult to access and use, leading to the exclusion of potential suppliers because of the imposed restrictions. A frequent example relates to the use of advanced electronic signatures which is considered as a strong user authentication method. Usually the process for obtaining a certificate is cumbersome and discourages suppliers (especially SMEs) who wish to use the eProcurement platform. Also, advanced electronic signatures are not always interoperable across different countries due mainly to a lack of mutual recognition..

Although security issues can be found in several other sections, two eProcurement Practices have been included in this section because they are directly related to the overall security of the system.

6.1.1 Utilisation of SSL to guarantee minimum communication security level

Different approaches have been followed by MS with regards to the "security versus interoperability" dilemma. However, a common security measure employed by all reviewed systems is the use of the SSL protocol for securing the communication between Web-browsers and servers. This is commonly considered as the necessary eProcurement Practice to guarantee the minimum level of system security.

Description	- Use Secure Socket Layer (SSL) for ensuring a minimum level of communication security
Functionality to be supported	- N/A
Implementation approach to follow	- SSL by using the Secure HyperText Transport Protocol (HTTPS) - Utilise the latest widely-used SSL standard of 128-bit encryption
System Module	All
Principles satisfied	Security
Risks	None
Input from	All systems

Good Practice #23 Utilisation of SSL to guarantee minimum communication security level

6.1.2 Secure communication between eProcurement and external systems

Security is an important issue for the Danish government. Denmark has established State Data Networks (SDNs), which are governmental networks connected to the common Internet gateway of the country. This network infrastructure is utilised by main public sector systems, including DOIP/DOIPEI. Therefore, the interconnection between the eProcurement platform and other governmental systems is performed under a very secure environment, which is ensured at the low-level, physical level.

Communication with suppliers is established through the Internet. However, suppliers that wish to enhance security of their integration with the eProcurement platform can establish Virtual Private Network (VPN) connections. A VPN connection creates a secure point-to-point communication between two parties, by using data encryption at the hardware level. The following eProcurement Practice is related to this concept.

Description	- Establish a low-level secured communication mechanism between an eProcurement system and other external systems (both public and private sector)
Functionality to be supported	- N/A
Implementation approach to follow	- Integrate systems through segregated networks (i.e. private networks) for guaranteeing high-level security - Establish VPNs between the eProcurement platform and other networks (a cheaper but still secure communication mechanism, utilising data encryption at the hardware level)
System Module	N/A
Principles satisfied	Security
Risks	None
Input from	DIOP/DOIPEI (Denmark), DPSM (France)

Good Practice #24 Secure communication between eProcurement and external systems

6.2 Electronic signatures

Electronic signatures are used for ensuring the proof of origin of electronically transmitted documents. Advanced electronic certificates are issued by Certification Authorities (CA) and are used for producing electronic signatures by their possessors. An electronically signed document guarantees the identity of the person who signed it. Furthermore, electronically signed documents ensure the consistency of the data of an electronically transmitted document. If a signed document is tampered, the signature is automatically invalidated. Therefore, the usage of advanced electronic signatures could be the ideal medium for ensuring the authenticity of tenderers and the integrity of data submitted by tenderers.

The drawback in utilising this technology is the limitations in interoperability. Each CA establishes its own methods for modelling this technology, usually abiding to local or national rules. The various CAs do not necessarily interconnect, and therefore suppliers that have a certificate from a CA are not necessarily trusted by another CA. This in turn means that a fully interoperable system needs to trust all CA, which is difficult to achieve. Furthermore, the time for obtaining the necessary software or hardware from a CA is usually lengthy and may require the physical presence of a supplier in the CA premises for approval. These issues make the utilisation of certificates and electronic signatures in an eProcurement system a significant hurdle for interoperability, potentially excluding suppliers from taking part in a business opportunity.

The European legislation does not impose the use of advanced electronic signatures leaving the decision of using them to the MS. The only requirement as imposed by EU is for electronic signatures to be compliant with the eSignatures directive. Nevertheless, even this directive does not guarantee the interoperability of electronic signatures.

Currently, MS have chosen either the route of interoperable but not fully secure-proof systems, or secure systems that exclude suppliers which do not have certificates from specific CAs.

6.2.1 Limited use of electronic signatures (only for critical activities)

In case a system uses electronic signatures, a good approach is to enforce the use of software certificates or smart cards only when a critical action in the system is performed.

The Danish DOIP/DOIPEI system, as analysed in Volume II (section 4.2.3), requests from users to enter their signature ID only when there are attempting to purchase or approve the procurement of goods or services, or generally perform other critical events. Therefore, users are not requested to enter their credentials on logon, when they are browsing through the eCatalogues in the systems. Similar approach has been followed in the French DPSM system, where electronic signatures are used by suppliers only for signing their tenders before submission.

The Italian eAuction Lotto 1 system (section Volume II - section 4.3.2) on the other hand utilises digital certificates stored on smart cards. However, users utilise their smart card only for their authentication and for confirming their bids at the end of an eAuction. During the eAuction and in order to establish a smooth bidding process, users before bidding, are required to enter a Personal ID Number. Through this number, Consip certifies that bids can be placed only by authorised users and in the same time ensures that the bidding process itself is quick and does not rely on the availability and response times of a third party.

The following eProcurement Practice refers to the sensitive issues of utilisation of electronic signatures.

Description	- Only critical activities should demand strong user authentication (Limited use of electronic signatures)
Functionality to be supported	- Suppliers electronically sign tender documents before submission - Contracting Authorities validate electronic signatures of submitted tenders - For eAuctions, suppliers use electronic signatures for confirming their winning tenders
Implementation approach to follow	- Define activities that are considered as critical events - Require the use of electornic signature credentials (software or smart card) only when critical events are performed
System Module	eTendering, eAwarding
Principles satisfied	Security
Risks	Equal Treatment, Interoperability (see discussion above)
Input from	DOIP/DOIPEI (Denmark), Lotto 1 (Italy), DPSM (France)

Good Practice #25 Limited use of electronic signatures (only for critical activities)

6.3 Time-stamping

The European legislation imposes strict rules with regards to the length of the eProcurement lifecycle. Especially for the submission of tenders during the eTendering phase, buying and supplying organisations need to always know what is the official time remaining before the closing of the tender submission period, as well as, the precise time a tender has been submitted to the Contracting Authority. Moreover, all activities in an eProcurement system may be audit-trailed and recorded to the official system logs, with the exact time they occurred.

To this end, MS can establish mechanisms for officially tracking time. Furthermore, they need to be in a position to communicate the time to suppliers through the front-end GUI of the system, as well as, utilise it in the automated system logs.

The reviewed systems do not utilise any mechanisms for obtaining official time from a third-party authority. The time is tracked through the system time of their servers and only a few implementations have established mechanisms for automatically synchronising time amongst all hardware devices. Although this might seem as a trivial area of eProcurement, the absolute synchronisation of time between all servers can ensure a good medium of traceability of events in the logs of each server. If logs of different servers have synchronised time, Contracting Authorities can easily follow events from one server to the other and generate meaningful reports. Moreover, attempts for tampering data can easily be identified, as for example an "update" entry in the logs of a database server, will need to be accompanied with a similar entry in the logs of the Web and Application servers. Obviously, such mapping can easily be achieved by the use of time-stamps in each server, which are synchronised.

As mentioned above, official time-stamping is essential for the submission of tenders. It is quite common for suppliers to submit their tenders shortly before the closing time of the eTendering phase. Therefore, only a system that utilises time from a certified official time authority can definitely know which tenders where submitted on time and which were submitted after the closing of the eTendering phase. For MS that utilise electronic signatures, and depending on the exact implementation, may be in a position to obtain the official time from the CA. However, this is a partial solution to the time-stamping aspect of eProcurement and therefore more systematic consideration of this issue is required for integrating to a certified time-stamping authority for concluding an official time-stamp for each system event.

6.4 Audit trailing

A cornerstone principle on eProcurement imposed by the EU legislation is that of traceability; the ability of the system to record all its interactions with users in system logs. The objective is to enhance the desired security aspect, as such logs can be analysed and provide legal evidence on system failures or irregular activities.

Almost all IT applications are capable of producing system logs. However, quite often system implementers do not consider system logs as an important output of the system. This results in human unfriendly logs, or occasionally incomplete in terms of what information they provide. Furthermore, an eProcurement system, being a complicated multi-tier software application, is usually constructed by many modules distributed on a number of servers. A proper logging mechanism should be in a position to merge logs from all modules and servers, and provide a unified "event log" to the user (administrator). A good event log needs to be easily constructible, and in such format to allow for further processing using a log analyser tool.

The following two eProcurement Practices are dealing with the aspect of audit trailing.

6.4.1 Matching logs from different modules and use a unified event log

A significant aspect that should be taken into consideration is the audit trailing of events that have occurred by approved users, authenticated using electronic signatures. The DOIP/DOIPEI system logs all activities for which electronic signatures have been utilised by storing in their logs not only the details of the activity, but also the User ID, Electronic Signature ID and the respective time-stamp. These logs can easily be unified into a common event log, allowing reviewers to follow the exact path of a competition/order through the system.

Description	- Match event logs from different eProcurement modules and create a unified event log
Functionality to be supported	- Trail procurement processes through the use of a common event log - Unify information created by the various eProcurement system modules and servers logs
Implementation approach to follow	- Logs created by different eProcurement system modules can provide complimentary information, which can assist a reviewer to follow the exact trail of a procurement process - Logs can be possible to be matched with each other in a simple way, creating a unified event log which can provide the full trail of system events as performed by users - Module and system logs can easily be matched and produce human-friendly information by the Time and User ID fields
System Module	All
Principles satisfied	Transparency
Risks	- Confidentiality may be breached in cases where unauthorised users of the Contracting Authority can review actions performed by suppliers, containing sensitive data (e.g. tender documentation)
Input from	DOIP/DOIPEI (Denmark)

Good Practice #26 Matching logs from different modules and use a unified event log

6.4.2 Safe storage of system logs

Another consideration for modelling the audit trailing mechanism is the safe storage of system logs. These logs record confidential data which can be accessible only by authorised personnel. A combination of the Norwegian and Danish implementation can produce a safe mechanism for tackling this requirement. The system logs of eHandel are "append only" files and do not allow the modification or deletion of stored information. Furthermore, the DOIP/DOIPEI system stores its logs in a server connected to a State Data Network (section 6.1). Therefore, the data that is recorded in a log cannot be altered in any way and only authorised personnel can access and process it. The following eProcurement Practice presents the concept of safe storage of system logs.

Description	- Store system logs in a secure environment - Allow access only to authorised personnel (i.e. system administrators)
Functionality to be supported	- N/A
Implementation approach to follow	- Only authorised personnel have access rights to module and system logs - Utilise "append only" mode for log files - Log files should be altered only by the system (no human intervention) - Logs created during submission of tenders should be accessible only for authorised Contracting Authority personnel - Storage of log files onto secure servers
System Module	All
Principles satisfied	Transparency
Risks	- Confidentiality may be breached in cases where unauthorised users of the contracting authority can review actions performed by suppliers containing sensitive data (e.g. bid documentation)
Input from	eHandel (Norway), DOIP/DOIPEI (Denmark), DPSM (France)

Good Practice #27 Safe storage of system logs

6.5 Reporting

The EU legislation requires MS to be in a position to report the ongoing or completed procurement competitions upon request from the EU. Reports should normally include details of the contract notice, the details of the admitted tenderers (including reasons for their selection), the rejected tenderers (and reasons), the successful tenderer (and reasons). Furthermore reports can provide details about the negotiation procedure, reasons for pausing an eAuction, reasons for not awarding a contract, etc. The majority of the reviewed systems can produce such reports, although some manual intervention and/or processing might be required.

However, apart from the standard EU reports, an advanced eProcurement system can allow for additional reporting capabilities. Suppliers usually wish to know their performance in one-off competitions and sales through their eCatalogues. Contracting Authorities want to understand their spending policy, as well as, the savings achieved through the use of the eProcurement system. Auditing authorities need to be in a position to study the information stored in the system logs and conclude on its compliant operation.

6.5.1 Generate reports on competitions using system event logs

The Norwegian eHandel system provides a module for the automated processing of system logs, offering the capability of generating reports on competitions and past user/system events. These reports contain information on both events that have taken place (usually stored in the system database) and activities that were attempted to be executed (failed events that are usually only stored in system logs). Furthermore, such reports can bring to light attempts to perform illegal activities, like tampering data and accessing confidential information. The following eProcurement Practice refers to the mechanism of generating reports using system logs.

Description	- Generate reports detailing activities that have taken place during competitions using system event logs
Functionality to be supported	- Creation of reports containing information on events occurred during the lifecycle of an eProcurement competition - The data source for the reports is the system logs
Implementation approach to follow	- Provide a tool for accessing, processing, and producing reports on activities based on the system logs - Support the analysis of the log information, so that the full audit trailing of a particular competition or a user's activities can be reported - Only authorised personnel should be able to gain access to this tool
System Module	All
Principles satisfied	Effectiveness
Risks	- Confidentiality may be breached in cases where unauthorised users of the contracting authority can review actions performed by suppliers containing sensitive data (e.g. tender documentation)
Input from	eHandel (Norway)

Good Practice #28 Generate reports on competitions using system event logs

6.5.2 Advanced statistical analysis on eProcurement data

Statistical analysis of eProcurement data is highly desirable. Both Contracting Authorities and suppliers can gain a great deal from utilising data-warehousing functionality. Contracting Authorities can understand their spending policy and savings generated from eProcurement, allowing for better spending policies and more efficient procurement competitions. Suppliers can benefit from obtaining accumulated data on their eProcurement participations.

The Danish and Norwegian administrations have opted for the implementation of an eCatalogue system first, exactly because they believed that the most important benefit for Contracting Authorities is to understand their spending through repetitive purchases. Therefore, the statistical analysis of data captured through the eProcurement systems was one of their primary objectives, assisting Contracting Authorities to understand and improve their spending policies.

Description	- Perform advanced statistical analysis - Assist Contracting Authorities to understand their spending policy - Assist suppliers to achieve better competition conditions
Functionality to be supported	- Provide data-warehousing functionality in order to exploit information contained in the eProcurement system - Capability to generate customisable reports
Implementation approach to follow	- Provide tools for analysing information for data generated through the repetitive purchasing of Contracting Authorities - Provide information to Contracting Authorities, assisting them to identify methods for improving their spending policies - Provide information to suppliers assisting them to identify their most popular and profitable products, best customers, etc.
System Module	All
Principles satisfied	Effectiveness
Risks	- Users only allowed to generate reports based on "their" set of data. - Information between Contracting Authorities cannot be shared, unless permitted by the legislation the system adheres to and without breaching the principle of confidentiality
Input from	DOIP/DOIPEI (Denmark), eHandel (Norway)

Good Practice #29 Advanced statistical analysis on eProcurement data

6.6 Virus protection & protection from malicious attacks

The issue of system disruptions because of virus attacks needs to be tackled by a state of the art eProcurement system. Activities taking place within the boundaries of the eProcurement system are relatively easy to control and are not considered as significant hurdles to overcome in terms of protection from computer viruses. However, an eProcurement system usually involves the execution of several activities outside of the context of the system.

In particular, during the eTendering phase, most reviewed eProcurement systems allow for the preparation of supplier tenders in document processing applications, usually using the MS Office software, or similar popular applications. This in turn means that a supplier computer infected by a virus can potentially generate tender documentation which includes dangerous computer viruses. Although it is relatively straightforward for a computer system to virus-check the tender documentation when received by a supplier, the complication arises with regards to the validity of a virus infected offer.

In theory, a virus scan constitutes the opening of tender document. This however is not allowed prior to the designated tender opening time, as tender documents are automatically locked and inaccessible. If the tender documentation is not virus-scanned at submission, may lead to an even more complicated situation. When opening a virus-infected tender document, which is always the eTendering deadline, the Contracting Authority may be given no other option but to consider the supplier tender document as invalid and disregard it in the evaluation process. Obviously, the re-submission of the tender documentation past the eTendering deadline is conflicting to the EU legislation.

Another major threat for Internet based systems is that of malicious attacks. In the recent years, there are numerous examples of malicious attacks to the most prestigious Internet systems. It appears that no matter the provisions in place, attackers can still achieve their aims in breaking into systems, or making them unavailable for a period of time. The responsible administration can have the necessary Service Level Agreement (SLA) in place with the hosting company, ensuring that the latest security measures are established, minimising the risk of such eventualities.

6.6.1 Virus check tenders upon submission

A number of systems employ the virus protection of supplier documentation by enforcing the automated scanning of submitted documents. This can indeed be compliant with the legislation depending on the way this virus scanning operation is modelled. The virus protection mechanism can be configured so that the virus reports do not provide any information with regards to the tender documentation. The reporting and audit trailing mechanisms of the virus scanner can only report whether a tender document is virus infected or not. Furthermore, virus infected files may be automatically deleted, or put to quarantine at a server location which ensures that the virus cannot infect other areas of the system and remain inaccessible. The following eProcurement Practice relates to the virus checking mechanism.

Description	- Automatic virus checking mechanism for submitted tenders - Automated notification of the corresponding supplier when tender documents are virus-infected
Functionality to be supported	- An automatic check of submitted tenders is performed and if a file is infected the system invalidates the supplier's tender - Provide an automated notification mechanism for informing the corresponding supplier that the submitted documentation is considered invalid due to the detection of viruses
Implementation approach to follow	- Perform an automatic virus check on submitted tenders - Virus infected files can be automatically deleted from the system, or put to quarantine at a server location which is secure and guarantees that the virus cannot infect other areas of the system - Nobody can gain access to infected documents - An automated notification can be sent to the corresponding supplier to inform about the virus-infected document - Audit trailing mechanism of the virus scanner can only report whether a tender document is infected, and not include confidential information
System Module	eTendering
Principles satisfied	Effectiveness, Security
Risks	- The virus scanning mechanism needs to be configured in such way to eliminate the recording of sensitive information in its system logs in order to ensure confidentiality
Input from	DPSM (France), EPSS (EU)

Good Practice #30 Virus check tenders upon submission

6.7 Interoperability

Interoperability is one of the biggest chapters of modelling eProcurement systems. An eProcurement system is not a stand-alone application which can achieve its objectives alone. Integration with other systems can significantly enhance the offered functionality and can accomplish the main goals in modernising the procurement process through the public sector. Furthermore, an eProcurement system needs to be widely accessible and available for all interested parties, allowing for the participation of suppliers, preserving the principle of equal treatment.

The interoperability of a system can be reviewed in terms of two categories: technical and procedural. The former is related to the technical capability of a system to integrate to other systems, while the latter refers to its ability to establish an open and widely accessible platform. The technical interoperability is reviewed in section 6.8, while this section considers procedural interoperability.

The procedural interoperability of a system is mainly related to how easily an interested party can gain access to it. However, eProcurement systems contain a lot of sensitive information subject to security and confidentiality rules and regulations.

6.7.1 Support multilingualism and parameterisation of the application

An aspect of the procedural interoperability is that of multilingualism and parameterisation. The nature of eProcurement systems implies its use in all geographic regions, which apart from different languages, includes the use of different currencies, date/time formats, monetary value formats, etc. An interoperable system needs to be in a position to assist all suppliers, local and foreign, in participating in a competition, irrespectively of their country of origin. Therefore, such parameterisation capabilities are desirable for achieving the procedural interoperability goal.

Currently, the Norwegian and Danish systems actively support multiple languages and allow suppliers to participate in competitions using the Norwegian, Danish, Swedish, Finnish, Icelandic, and English language. Furthermore, it is not only the front-end of a system that supports different character set, but also all other layers of their systems. Furthermore, the Norwegian eHandel system and the French DPSM eCatalogues module support some parameterisation, by allowing users to select the currency they wish to work with.

Description	- Provide multilingualism support and an easily parameterised GUI
Functionality to be supported	- Flexible GUIs to allow parameterisation based on user preferences - Back-end systems to support multiple languages
Implementation approach to follow	- Support multiple languages, allowing use of different character sets - Parameterisation of the GUI by users including: o Currency o Date/time format o Monetary value format o Units of measure
System Module	All
Principles satisfied	Equal treatment, General availability
Risks	None
Input from	eHandel (Norway), DOIP/DOIPEI (Denmark), EPSS (EU), DPSM (France)

Good Practice #31 Support multilingualism and parameterisation of the application

6.8 Integration Capabilities

The integration of different eProcurement systems and applications significantly increase their efficiency in public procurement. An advanced integration capability used in Norway and Denmark, is the integration with supplier systems in order to automatically obtain eCatalogues data. Non-automated eCatalogues can lead to discrepancies and errors. Furthermore, the conversion of one catalogue format to another is time consuming. The Norwegian and Danish implementation can minimise the human effort required, as the automated mechanisms they have realised can achieve necessary format/data conversions. In addition to that, eHandel can integrate with supplier warehousing systems, allowing for Contracting Authorities to check a supplier's stock real-time.

Another version of the above integration is the remote access ("punch-out") capability of the Scottish PECOS system, which can access a supplier Website and directly obtain all catalogue information. Furthermore, an application which does not achieve integration, but can certainly reduce the effort for maintaining eCatalogues, is the eCatalogue Converter from UK/Scotland (Volume II – section 4.4.2).

It is interesting to note that significant effort is currently being dedicated throughout Europe in identifying message transfer standards which can assist implementers in creating generally interoperable systems. The Danish administration is using OIOXML UBL, Norway is utilising xCBL, the UK government has recently established their UKGOV XML standard, while the EC is currently running the "eProcurement XML Schema" project, attempting to specify generic eProcurement XML Schemas to be made available throughout Europe for current and future systems.

Nevertheless, offering integration capabilities to suppliers, needs to be treated with great care by public administrations. The integration of an eProcurement system with supplier systems usually involves significant investment. Some SMEs may not be in a position to incur the necessary expenses for such integration, and therefore indirectly give an advantage to their competitors. Furthermore, necessary procedures need to be defined for supplier catalogue maintenance. An advanced eProcurement system needs to make sure that eCatalogues are only updated according to the specifications agreed between Contracting Authorities and suppliers (i.e. framework agreement for product price, quality, etc.). Moreover, monitoring policies need to be defined by Contracting Authorities in order to ensure that all procedural guarantees are respected, for example when purchasing through automated eCatalogue systems.

Although advanced integration capabilities of an eProcurement system can offer great benefits, at the same time they must be designed in such way in order to ensure the system meets its primary objectives: equal treatment and transparency.

The following two eProcurement Practices relates to the integration capabilities of an eProcurement system.

6.8.1 Integration with financial systems

Significant benefits can be achieved by integrating an eProcurement repetitive purchasing system to the financial systems of Contracting Authorities and suppliers. Such integration can facilitate automated invoicing and payment, through constant status monitoring and automated settlement processes. Such integration can achieve significant benefits for both buyers and suppliers, not only in terms of time-saving, but also by allowing the error-free storage and analysis of Contract Authorities' spending and suppliers' sales.

Description	- Integrate repetitive purchasing systems with supplier and Contracting Authority financial back-office systems
Functionality to be supported	- Automated uploading of supplier eCatalogues - Order status monitoring - Electronic invoicing by suppliers - Electronic payment - Real-time checking of supplier stock by Contracting Authorities
Implementation approach to follow	- Establish a protocol of communication between the eProcurement system and financial systems - Automatic conversion of eCatalogues to the necessary format
System Module	eInvoicing, ePayment
Principles satisfied	Effectiveness, Interoperability
Risks	- Security and confidentiality issues can be taken into account when establishing a communication with financial systems
Input from	eHandel (Norway), DOIP/DOIPEI (Denmark)

Good Practice #32 Integration with financial systems

6.8.2 Establishment of a transactional hub to facilitate communication between different systems

For achieving the desired integration, there can be well-established message transfer standards, as well as, secure means of communication. To tackle this issue, the Danish administration developed a transaction hub, called Business Transaction Service (BTS); a module of DOIP/DOIPEI specifically designed for routing information and converting the data format if required. Through this mechanism, Contracting Authorities and supplying organisations are not required to invest on modifying their existing systems for achieving system integration. Instead, the routing and format conversion rules need to be defined within BTS and achieve integration relatively easily.

In addition to the existing BTS system, OGC of the UK have recently initiated the Zanzibar project, with similar objectives to BTS. The following eProcurement Practices is derived from this approach.

Description	- Establish a transactional hub between the eProcurement system and other Contracting Authority or supplier systems
Functionality to be supported	- N/A
Implementation approach to follow	- Use transaction hub for converting format of transferred messages in the appropriate data format of the destination system - Operate as a routing medium for transferred messages - Employ a full audit trailing facility, inbound and outbound queues guaranteeing the delivery of messages and advanced security features
System Module	All
Principles satisfied	Effectiveness, Interoperability
Risks	- Security and confidentiality issues can be taken into account when establishing a communication between systems
Input from	DOIP/DOIPEI (Denmark), Zanzibar (UK)

Good Practice #33 Establishment of a transactional hub to facilitate communication between different systems

6.9 Electronic document standards

The topic of document standards is related to the equality of treatment and the interoperability needs of eProcurement systems. Public sector eProcurement systems need to be openly available and easily accessible by all. This in turn can be translated to suppliers being in a position to use their own computer programs and IT infrastructure in order to use an eProcurement system. When preparing tender documentation, suppliers cannot be forced to use a specific software program or hardware set-up, unless the cost is low and generally acceptable by all.

Supplier size and IT-awareness can vary significantly, enforcing therefore the use of a specific product and operating system, which can be discriminatory. The following eProcurement Practice refers to this aspect.

6.9.1 Support of all widely used electronic document standards

The commonly used electronic document standards throughout the European systems seem to be:

- **Portable Document Format (PDF):** is very commonly used in the Internet, as the size of documents constructed in PDF is usually smaller in relation to other document formats, making it easy to download through a simple modem connection. PDF Viewers are available at no cost to the general public; however the generation of PDF documents requires the purchase of the PDF Writer software. PDF files are well-protected from computer viruses.
- **HyperText Markup Language (HTML):** is a text based format, which can be generated through sophisticated HTML Editors (freeware), or even a simple Text Editor. It can support most features of a "normal" document like tables, figures, lists, etc. and can be viewed by cost-free applications like Web-browsers. HTML appears to be one of the most interoperable formats currently used.
- **Rich Text Format (RTF):** is a method of encoding formatted text and graphics for easy transfer between applications, which is portable between different operating systems,

including MS-DOS, Windows, OS/2 and Macintosh. RTF documents can be created and viewed by many applications, the more sophisticated ones necessitating licensing costs.

- **MS Word (DOC):** is commonly used as MS Word is probably the most popular word processing application today. Nevertheless the creation and viewing of DOC format requires the purchase of the MS Office software. A number of freeware applications are available which can create, open and modify documents in DOC format, however not all of these application support all formatting features used in DOC.
- **MS Excel (XLS):** similarly to DOC, XLS is the document format for MS Excel, the MS Office application for creating spreadsheets, charts, etc.

The following eProcurement Practice promotes the support of all electronic document standards.

Description	- Capability to support all widely-used electronic document standards
Functionality to be supported	- N/A
Implementation approach to follow	- Allow suppliers to choose from a wide range of options of document standards - Suppliers need to be informed of the complete list of formats they are allowed to select from - Pre-stated supported document standards may also detail the application versions which can be used for the preparation of tender documentation
System Module	All
Principles satisfied	Effectiveness, Interoperability, General availability
Risks	None
Input from	All

Good Practice #34 Support of all widely used electronic document standards

6.10 Software adaptability

An important quality aspect of all software systems is the capability to adapt to the eProcurement business logic, and its potential future modifications. In particular, users of eProcurement systems can benefit a great deal by systems developed in a modular way, allowing them to define the exact operation of the systems depending on their specific needs.

As identified during the analysis of the reviewed EU systems, a service that can significantly assist Contracting Authorities to conduct valid competitions and achieve the desired objectives quickly and efficiently, is the provision of a collaborative environment. The eNotification phase requires a certain amount of documentation to be created and published. Such documentation needs to contain all details of the competition, the product/service/work specification to be procured, pre-requisites for participation, pre-stated criteria and other procurement details. Therefore, the notification documentation can introduce significant delays each time a procurement competition needs to take place, as potentially many officers and/or departments of the Contracting Authority need to be involved, following their internal bureaucratic validation and approval path.

6.10.1 Workflow management for assisting the preparation of call documentation

Some operational and under development systems offer a collaborative environment which assists Contracting Authorities in the process of creating the notification documentation. Flexible workflow processes allow for the drafting, validation and approval paths within the Contracting Authority, which can reduce delays, inconsistencies and other paper-related issues. Contracting Authorities define their own workflow processes depending on the value of the contract and/or the goods or services to be procured. Such online modelling can furthermore assist Contracting Authorities in re-engineering their internal bureaucratic flows, allowing for their optimisation.

Moreover, pre-defined document templates can assist Contracting Authorities in creating their call documentation, as well as, educating their personnel on the content that is required for each contract document.

Description	- Workflow management for establishing approval paths - Contract document templates for assisting the preparation of the call documentation
Functionality to be supported	- Preparation of call documentation through the use of document templates - Support of different user profiles with drafting/approval roles - Approval and validation of user activities following workflows
Implementation approach to follow	- Contract document templates used for educating public sector officers to the number of documents required for conducting a fully compliant competition, as well as, the content of each document - Contract document templates can include specifications of the required goods/services/works, procurement objectives, pre-stated criteria and other parameters - Collaborative environment, where the internal procedures of the Contracting Authority can be modelled into flexible system workflows - Establish workflows to optimise the approval paths followed (from drafting a contract document to its final approval)
System Module	eNotification
Principles satisfied	Effectiveness
Risks	None
Input from	eSourcing Services (UK), ehandel eSourcing (Norway), DPSM (France), SYSLOG Market (EU)

Good Practice #35 Workflow management for assisting the preparation of call documentation

6.10.2 Modelling procurement competition phases as a series of eProcurement events

The approach used by ehandel eSourcing (Norway) for designing eProcurement competitions is highly adaptable. An eProcurement competition comprises a number of sequential activities including notifications, auctions, submissions, pre-evaluations, evaluations, etc. The modelling of eProcurement competitions as a sequential execution of events, allows administrations to define the exact procedure to follow for each procurement competition. eProcurement events are treated as "components" which the Contracting Authority can select, prioritise and configure, building the exact procurement process to be followed.

Description	- Model the different procurement competition phases as a sequential execution of distinct eProcurement events ("block components")
Functionality to be supported	- Create an eProcurement competition by selecting and prioritising the different "block components" which will be executed sequentially
Implementation approach to follow	- Model each eProcurement phase as a collection of distinct "block components" (notification events, submission events, evaluation events, eAuction events, etc.) - Allow Contracting Authorities to configure their own eProcurement competition by selecting the sequential execution of "block components" to be followed - Assist buyer users in defining competitions that are compliant with the EU legislation - Define "competition templates", which re-create the complete eProcurement process according to the legislation, using the appropriate "block components" (e.g. "Competition templates" can be: Open competition with auction, Restricted competition without auction, Negotiated competition without notification, etc.)
System Module	eNotification
Principles satisfied	Effectiveness
Risks	None
Input from	ehandel eSourcing (Norway)

Good Practice #36 Modelling procurement competition phases as a series of eProcurement events

6.11 Further analysis of eProcurement Practices related to technical aspects

This section summarises the results derived from the review of technical eProcurement Practices. Table 5 lists the main principles satisfied by them. Potential risks from the implementation of technical eProcurement Practice are also displayed in this table (small triangles).

No	Technical eProcurement Practices	Equal Treatment	Transparency	Effectiveness	Interoperability	Security	General availability	Confidentiality
23	Utilisation of SSL to guarantee minimum communication security level					✓		
24	Secure communication between eProcurement and external systems					✓		
25	Limited use of electronic signatures (only for critical activities)	?			?	✓		
26	Matching logs from different modules and use a unified event log		✓					?
27	Safe storage of system logs		✓					?
28	Generate reports on competitions using system event logs			✓				?
29	Advanced statistical analysis on eProcurement data			✓				?
30	Virus check tenders upon submission			✓		✓		?
31	Support multilingualism and parameterisation of the application	✓					✓	
32	Integration with financial systems			✓	✓	?		?
33	Establishment of a transactional hub to facilitate communication between different systems			✓	✓	?		?
34	Support of all widely used electronic document standards			✓	✓		✓	
35	Workflow management for assisting the preparation of call documentation			✓				
36	Modelling procurement competition phases as a series of eProcurement events			✓				

Table 5: Coverage of the EU legislation principles by the technical eProcurement Practices

7 eProcurement Practices concerning operational aspects

This section analyses the operational procurement aspects of the reviewed procurement systems. It considers operational aspects that provide services to Contracting Authorities and suppliers in order to effectively and fairly conduct/participate in competitions, as well as, plans that can set the roles and actions in case of system failures. Five categories have been identified for grouping eProcurement Practices related to operational aspects:

- **Operational support to participating organisations:** Methods and policies employed by eProcurement National eProcurement Authorities in order to assist both Contracting Authorities and suppliers in resolving issues related to the fine operation of the eProcurement platform
- **Quality of content:** Mechanisms for ensuring the quality of provided information
- **System implementation approach:** Methods for developing a new eProcurement system
- **Volume capacity:** Issues related to the management of large volumes of exchanged information between all involved parties in eProcurement
- **Complaint procedures:** Methods for raising complaints and management of disputes

7.1 Operational support to participating organisations

This section deals with procedures and policies of National eProcurement Authorities in order to assist both Contracting Authorities and suppliers in dealing with the various issues related to the fine operation of the eProcurement platform. Considered aspects here include legal advice, consulting, technological support and any other forms of assistance provided to the involved parties.

7.1.1 Provide legal support to participating organisations

The OGC of the UK provides legal support to Contracting Authorities, allowing inexperienced and/or small contracting authorities to conduct fair and transparent competitions. Currently, the provided legal support focuses on the way eAuctions are conducted, providing legal consulting during the auction event. Furthermore, while executing an auction event, the OGC offer Q&A and helpdesk support to all suppliers, in order to assist with any technical or other problems they may face (Volume II – section 4.3.1). Nevertheless, this operation without the provision of legal support can lead to unfair competition, invalidating the process.

Description	- Offer legal support to Contracting Authorities for conducting fairer and more transparent competitions - Offer assistance to suppliers in order to help them better understand the legal framework of Public eProcurement
Functionality to be supported	- N/A
Implementation approach to follow	- Ensure that valid competitions are conducted according to the EU regulations of equal treatment, non discrimination, transparency and confidentiality. - Offer legal support during the specification and the progress of a competition
System Module	All
Principles satisfied	Effectiveness
Risks	None
Input from	OGC (UK)

Good Practice #37 Provide legal support to participating organisations

7.1.2 Organise training events simulating the real competition environment

It is essential that both Contracting Authorities and suppliers are trained in using an eProcurement system. Currently, almost all reviewed administrations offer training courses, through which the users of the system can get familiarised with the available functionality and participate in competitions with the complete knowledge of the system.

An interesting activity of the Italian administration Consip, followed also by the French MINDEF, relates to the training of suppliers for the hosting of eAuctions. All suppliers, prior to an eAuction event, are invited to participate in two training auction events, where the exact details of the real eAuction (including auction type, evaluation formula, bidding fields, etc.) are prepared by the Contracting Authority. During these training events, the real competition is simulated through the competing suppliers. All participants are given the opportunity to understand the auction details, experiment with the evaluation formula and comprehend its function, and appreciate the full functionality offered by the system.

Description	- Organise training sessions that simulate the real competition conditions - Invite all involved parties to participate
Functionality to be supported	- Hosting of "virtual" competitions for training purposes
Implementation approach to follow	- Hosting of training events to simulate the real procurement event can assist suppliers to get familiarise with the system - Suppliers not only get trained on the general use of the system, but also experiment with the exact configuration options of the forthcoming competition
System Module	All
Principles satisfied	Equal treatment, Effectiveness
Risks	None
Input from	Consip (Italy), MINDEF (France)

Good Practice #38 Organise training events simulating the real competition environment

7.1.3 Offer consultancy services to Contracting Authorities

Consultancy is another service which almost certainly can add value to procurement competitions. Contracting Authorities that are not accustomed to the new procurement procedures can significantly benefit from a consultancy service, which can assist them to understand the new rules and regulations. Consultancy services can assist Contracting Authorities to plan their competition is such way so that they achieve maximum benefits. The nature of an eProcurement competition heavily depends on the type of the commodities or services to be procured. Furthermore, the compilation of all notification documents can be a substantial hurdle for inexperienced buyers. Another serious issue is the definition of evaluation formulae for eAuctions, which require thorough analysis before being formalised.

In order to assist Contracting Authorities to overcome these issues, the technology providers of OGC offer consultancy services. Although these services are offered for a certain fee, the effective analysis and planning of a competition can achieve significant savings and increase quality of the final products or services procured. Therefore, OGC believes that the available consultancy services can save significant amount of money for competitions of inexperienced public sector buying organisations.

Description	- Offer consultancy services to Contracting Authorities in order to accustom them with the new procurement environment - Assist Contracting Authorities in planning effective competitions
Functionality to be supported	N/A
Implementation approach to follow	- Cover all areas foreseen by the EU legislation suited to the purchasing needs of the Contracting Authority - Offer assistance in the planning of procurement competitions - Analyse the exact requirements of the Contracting Authority - Formalise Contracting Authority's requirements into eNotification documents - Define evaluation formulae and the overall procurement strategy to be followed
System Module	All
Principles satisfied	Effectiveness
Risks	None
Input from	OGC (UK)

Good Practice #39 Offer consultancy services to Contracting Authorities

7.2 Quality of content

This section covers the aspect of quality of content stored in an eProcurement system.

7.2.1 Assure quality of supplier eCatalogues

The Norwegian administration (GAS) has given significant attention to the quality of data that is imported to the eHandel eCatalogues system. In particular, the view of the administration is that a good system can provide adequate functionality for improving the internal procedures of the Norwegian public sector, reducing in the same time costs involved. However, this can only be achieved by the high quality of content included in the system. GAS has ensured that their technology provider offer a cost-free service to the participating suppliers, for performing quality assurance to suppliers' catalogues. This is conducted on a frequent basis and feedback is given to suppliers for improving their catalogues.

Each electronic catalogue is evaluated in five different levels:

- Categorisation
- Usage and quality of images
- Product name
- Product description
- Product attributes

Each level is evaluated by the score of 0 (inadequate quality), 1 (adequate quality) and 2 (state-of-the-art). Following this simple procedure, the Norwegian administration can assist suppliers in providing high-quality catalogues to the system. This practice can ensure that all suppliers are given an opportunity for equal treatment, as even smaller SMEs will be guided in constructing appropriate catalogues, ensuring their products are marketed and can be located through the system's search engines in a satisfactory way.

Furthermore, high-quality of eCatalogues can ensure that products of a given supplier are not "over-exposed" to the search engine of eHandel. This can ensure that when a Contracting Authority is trying to locate a certain type of product, s/he will not be presented with all products with similar description (i.e. when searching for "laptop", will not be presented with personal computers).

Description	- Perform quality assurance to supplier eCatalogues
Functionality to be supported	- Well described products can be easily found by search engines and are not "over-exposed" to a wide range of searches - Effective use of coding hierarchy can significantly assist Contracting Authorities to locate desired products in supplier eCatalogues
Implementation approach to follow	- Establish a methodology for eCatalogues evaluation - Evaluate catalogues in terms of the established methodology - Establish a procedure by which all eCatalogues are reviewed and evaluated on a frequent basis
System Module	N/A
Principles satisfied	Equality of treatment, Effectiveness
Risks	None
Input from	eHandel (Norway)

Good Practice #40 Assure quality of supplier eCatalogues

7.3 Definition of Operational Requirements

When defining the functional requirements of their eProcurement system, Contracting Authorities may also specify their requirements for the operational performance of the system. These requirements may include minimum downtime in case of system failures, technical hotline support from the hosting providers, number of maximum/minimum concurrent users requests to the system, etc.

7.3.1 Define level of services with the technology providers

The eProcurement software solution needs to be very well implemented in order to manage with the heavy load of transferred data during certain time. The hosting servers have to be powerful enough to handle the increased volume of transactions. The network architecture needs to be capable enough to avoid traffic congestions. The complete software and hardware environment needs to be implemented and configured in an optimum way, ensuring no volume capacity faults. All these parameters may be specified in Service Level Agreement (SLA) between the Contracting Authority and the technology provider(s).

Description	- Establish SLAs that define the acceptable level of operation of the eProcurement platform by the technology providers
Functionality to be supported	N/A
Implementation approach to follow	- Establish SLAs which precisely define the operation mode of the eProcurement platform by the hosting company - The SLA may include: o Response times in case of normal operation and system failures o Responsibilities of each sub-contractor involved (i.e. responsible for the software, hardware, network infrastructure, Internet connection, etc.) o Bandwidth available (especially during the closing of an eTendering phase) - The SLA (or part of it) may be communicated to all Contracting Authorities and suppliers participating in a competition, allowing them to understand the available provisions
System Module	All
Principles satisfied	Effectiveness, General availability
Risks	None
Input from	All MS

Good Practice #41 Define level of services with the technology providers

7.4 Volume Capacity

A common issue with eProcurement is the submission of tenders very close to the eTendering deadline. Suppliers usually define their best offer for a business opportunity until the closing hours of the eTendering phase and they submit their offers almost simultaneously a few hours or even minutes before the closing time. This in turn can potentially generate difficulties, as the IT infrastructure needs to cope with the concurrent submissions, without creating unavailability or disruption problems.

7.4.1 Policy for extending eTendering deadline due to volume capacity problems

The reviewed MS do not seem to have mature, robust methods for dealing with volume capacity issues during competition. The reviewed administrations are either definite that no such failure can occur to their implementation, or they deal with the problem if and when it occurs on a case-by-case basis. The following eProcurement Practice is related to this aspect.

Description	- Establish methods for dealing with volume capacity problems during the closing time of the submission phase
Functionality to be supported	- Server/network traffic monitoring tools
Implementation approach to follow	- Establish submission deadline extension policies, which detail precisely the conditions and actions to be taken when system failures occur during the closing stages of eTendering, due to volume capacity problems - Use monitoring tools to closely supervise the behaviour of the system (residing servers, underlying network functioning) in order to identify potential and actual problems and be in a position to take appropriate actions - If an extension to the submission phase is given, all participating suppliers need to be promptly notified of the new deadline
System Module	eTendering
Principles satisfied	Equal treatment, Transparency, General availability
Risks	None
Input from	DTC (UK/Scotland)

Good Practice #42 Policy for extending eTendering deadline due to volume capacity problems

7.4.2 Implementation of a two-phased submission process

An interesting idea employed by the French DPSM system is the utilisation of electronic signatures for reducing the network load during the eTendering phase. The French system has attempted to overcome the common problem of large volumes of data transferred during the closing period of submitting tenders, by providing a two-phased submission process. During the first phase, the tenderer is required only to submit the hash value of the electronically signed tender documents, while in the second phase the tenderer submits the tender documents themselves. During the second phase, the tenderer is required to submit the tender documents within 24 hours after the eTendering deadline. A tender may comprise more than one documents, which need to be signed by the supplier following the same process.

Through this mechanism, suppliers are required to upload small amounts of data during the closing time of the tender submission period, reducing the possibility of technical failures due to overloading the volume capacity of the system. This mechanism forms the following eProcurement Practice.

Description	- Implementation of a two-phased submission process for dealing with volume capacity issues during the closing time of eTendering - Firstly, supplier only sends the hash value of the electronically signed document - Subsequently, tender document itself is submitted by supplier, within a defined time-frame after the expiration of the eTendering deadline
Functionality to be supported	- Supplier submit hash value of the tender document before eTendering phase deadline - Submission of the tender document itself within a pre-specified time frame after the expiration of the bidding deadline
Implementation approach to follow	- Model a mechanism that can accept tender documents in two phases: o First: submission of the hash value of the document o Second: submission of the document itself - Verify that the document submitted during the second phase corresponds to the hash value sent in the first phase
System Module	eTendering
Principles satisfied	General availability
Risks	- The interoperability issues related to the electronic signatures need to be taken into account
Input from	DPSM (France), eContratacion (Spain/Basque)

Good Practice #43Implementation of a two-phased submission process

7.4.3 Allow the downloading of submitted tenders before eTendering deadline

Another interesting approach applied to the French DPSM system, deals with the volume of transferred data is the downloading of encrypted tenders. It has been observed that for opening the submitted tenders, the awarding committees have to firstly download all tender documentation and decrypt it before being able to read the contents. This obviously increases the network requirements of the system, as usually the tender documentation is a collection of large documents. Furthermore, the downloading process is longwinded and time consuming. To address this issue, DPSM allows Contracting Authority officers, who are responsible for the management of the tender workspace, to download the encrypted tenders and store them in the awarding authority's local system. Tenders can be decrypted only by the private key of the president of the awarding committee, which can be obtained only after the submission closing time.

Description	- Offer the possibility to the Contracting Authorities to download tenders before the expiration of the eTendering deadline - Reduce volume requirements during the opening of tenders
Functionality to be supported	- The purchasing officer is able to download uploaded submitted tenders to his/her own physical location at any time - Tenders remain locked (i.e. encrypted) and inaccessible until the eAwarding phase
Implementation approach to follow	- Authorised users can download encrypted tenders before the eTendering deadline expires - Encrypted tenders can not be decrypted by anyone except the authorised personnel only after the expiration of the eTendering deadline
System Module	eTendering, eAwarding
Principles satisfied	General availability, Security
Risks	None
Input from	DPSM (France)

Good Practice #44 Allow the downloading of submitted tenders before eTendering deadline

7.5 Complaint Procedures

It is not uncommon for suppliers to express their belief that a procurement competition can be considered as invalid, because it did not take place according to the ruling legislation. MS usually have existing bodies which deal with complaint procedures, initiated by suppliers.

The operation of such bodies can obviously become a lot easier in comparison to non-electronic procurement, due to the audit trailing capabilities of such systems. All activities of eProcurement phases are recorded and stored into the system, allowing for a very detailed analysis of past or current competitions. However, the government bodies resolving complaints need to be educated in the operations and data they can now obtain and furthermore new resolution procedures may need to be established.

7.6 Further analysis of eProcurement Practices related to operational aspects

This section summarises the results derived from the review of the most useful operational eProcurement Practices. The analysis in Table 6 lists the main principles satisfied by them. Potential risks from the implementation of operational eProcurement Practices are also displayed in this table (small triangles).

No	Operational eProcurement Practices	Equal Treatment	Transparency	Effectiveness	Interoperability	Security	General availability	Confidentiality
37	Provide legal support to participating organisations			✓				
38	Organise training events simulating the real competition environment	✓		✓				
39	Offer consultancy services to Contracting Authorities			✓				
40	Assure quality of supplier eCatalogues	✓		✓				
41	Define level of services with the technology providers			✓			✓	
42	Policy for extending eTendering deadline due to volume capacity problems	✓	✓				✓	
43	Implementation of a two-phased submission process				?		✓	
44	Allow the downloading of submitted tenders before eTendering deadline						✓	

Table 6: Coverage of the EU legislation principles by the operational eProcurement Practices

8 Conclusion

The analysis performed in the context of the current report identified 44 interesting eProcurement Practices, resulting by the review of 21 European procurement systems. These practices were classified into four categories, covering all aspects of an eProcurement programme: organisational, procedural, technical and operational.

Table 7 highlights some of the most useful Procurement Practices, which if implemented can contribute strongly to the functionality and operation of public procurement systems.

Organisational	**Establishment of a transparent contracting relation plan (eProcurement Practice #1):** – Assist public administrations in joining eProcurement – Provide confidence by clearly defining roles and responsibility for all involved parties, through a well established contractual framework
	Supplier adoption programme (eProcurement Practice #4): – Educate suppliers in public eProcurement and encourage them in participating in competitions – Assist suppliers in modifying their internal procedures for benefiting from eProcurement
Procedural	**Use of electronic messages to automate publication to OJEU (eProcurement Practice #5)** – Establish integration with OJEU for automated publishing of contract notices above the EU threshold
	Offer multiple methods of registration (eProcurement Practice #9) – Allow users to select simple or advanced (utilising electronic certificates) registration process
	Moderate Q&A session to ensure confidentiality (eProcurement Practice #11) – Support Questions and Answers sessions – Employ mechanisms for ensuring confidentiality
	Assist suppliers during submission through user-friendly GUI (eProcurement Practice #15) – Design Graphical User Interfaces which assist users in understanding the full functionality of the system – Use colour coding, animations and other visual effects for informing users of significant events

Technical	**Utilisation of SSL to guarantee minimum communication security level (eProcurement Practice #23)** – Use Secure Socket Layer for encrypting data transmitted from the system servers to user PC, and vice versa
	Matching logs from different modules and use a unified event log (eProcurement Practice #26) – Ensure system logs of the audit trailing module can produce meaningful reports
	Support of all widely used electronic document standards (eProcurement Practice #34) – Clearly define applications and versions that can be used by suppliers for completing their offers
Operational	**Organise training events simulating the real competition environment (eProcurement Practice #38)** – Invite all qualified supplier to participate in training events – Allow all parties to get familiarised to the real competition environment, by utilising the real competition parameters (i.e. evaluation formula)
	Define level of services with technology providers (eProcurement Practice #41) – Establish Service Level Agreements with all technology providers
	Allow the downloading of submitted tenders before eTendering deadline (eProcurement Practice #44) – Reduce volume requirements during the opening of tenders – Ensure confidentiality by encrypting tenders

Table 7: Highly recommended eProcurement Practices

One of the important conclusions of the study is that no public eProcurement system fully supports the new EU public procurement directives. The existing systems have been conceptualised, designed, and implemented prior to the establishment of the current EU public procurement legislation. Hence, despite their sophistication and advanced functionality, they do not fully operate according to the legislation. The new directives offer an opportunity to MS to cooperate in homogenising their approaches to eProcurement. To achieve this goal, the creation of a common conceptual view of the required procedures needs to be completed. The conceptual view will then be possible to be transposed to functional requirements and technical specifications, facilitating a solid basis for implementing systems fully compliant with the directives.

Similarly, MS have followed different approaches on the security, and in particular for user authentication and authorisation. Some MS have focused heavily in establishing secure environments through the use of advanced electronic signatures and smart cards, while others have opted for simpler security measures. The drawback of the former approach is the limitation in interoperability, while the later approach can lead to less secure systems. Security and interoperability are key principles of the new directives. Various projects are underway related to security and interoperability in order to identify methods for establishing IT systems that satisfy both principles. Further work is necessary to reach workable solutions across the EU internal market to avoid barriers to cross-border electronic public procurement.

Another important finding concerns the technical implementation of all reviewed systems. Currently, all operational eProcurement systems are based on commercial products offered by vendors, usually customised to some degree. Although the commercial systems selected by MS are very advanced, they have resulted in software-driven rather than legislation-driven systems. The customisation of commercial products is usually costly, while their usage is usually bound to specific hardware technologies, vendors, software licences, etc. MS need to focus in establishing eProcurement systems which fully support the functional requirements required by the EU legislation. The use of Open Source Software technologies can provide a method for MS to share tools and solutions with reduced costs. The exchange and sharing of common tools, openly available components/modules, and common software development approaches can assist operators in implanting eProcurement systems in a cost-effective manner.

Throughout the current analysis, public administrations confirmed the achievement of significant benefits from the implementation of eProcurement solution for both public and private sector participants. The organisation of more transparent competitions and the creation of a more attractive procurement environment encourage suppliers to participate and compete for new business opportunities. The ongoing development of eProcurement systems is expected to offer new functionality, thus achieving additional savings. The continuous research in establishing generally available, secure and interoperable systems is expected to encourage more suppliers to participate in public eProcurement competitions.

Cross-border coordination and contribution to European projects, similar to the current project, is necessary for establishing pan-European standards and common EU approaches to eProcurement. Such European initiatives can assist MS to reduce implementation/ongoing costs on eProcurement, by sharing experiences and identifying solutions to common eProcurement issues.