To whom it may concern

Subject/objet Request for Information – ‘Document-Centric Portal’

The Information Systems Department (OPS-I) of the European Space Agency is planning to launch an invitation to tender to implement a ‘Document-Centric Portal’ (DoCeP) in 2005.

To this end, the Department has developed a vision for such a portal, which is detailed in Appendix B of this Request for Information (RFI).

As part of our ongoing effort to assure potential bidders of our interest in their participation in and understanding of the ESA tendering process for this ‘Document Centric Portal’ project, we would like to start a mutually beneficial exchange of information on this subject. This will facilitate the construction of the project business case and the preparation of the tender itself, and hopefully provide you with a better basis for preparing a realistic and competitive bid.

The exchange of information is intended to clarify and prepare the competition that is aimed at selecting a prime contractor (system integrator and/or service provider) that will manage the selection of the Enterprise Content Management/Smart Enterprise Suite (ECM/SES), the phased implementation and integration of the DoCeP, and ensure the overall service delivery to the Agency.

The Agency is looking at two different procurement approaches (classical “project” approach, “service” approach), which are described in Annex C.

Based on market intelligence and its own research, the Agency has tentatively shortlisted the following ECM/SES suites for implementing the DoCeP (in alphabetical order):

- EMC/Documentum
- FileNet P8
- Hummingbird Enterprise 2004
- OpenText LiveLink 9

Note that the choice of one ECM/SES will be up to the prime contractor when answering to the tender; the selection (which is not limited to the Agency’s
shortlisted products) should – at tender stage - be well justified and based on the requirements of ESA.

For the purpose of this RFI, we would be grateful if you could prepare and provide us with the following information:

1. Standard documentation that you have readily available for the services required by ESA, in particular:
   - Service Level Agreements
   - Quality of service metrics and methods of service measurement
   - Service catalogues

2. A short list of existing customers, that we may contact, and to whom you provide services the same as, or comparable to, those anticipated by ESA.

3. Answers to the questions in Annex E.

4. Any additional information in respect to your activities or approach that you feel will aid us.

5. Any question or clarification that you deem necessary in order to prepare your company for the tender process. Should you require any information at any stage prior to the formal tendering process then now is the time to put forwards such requests (e.g., on the tendering procedure).

6. Finally, we would like to know if your company is ready to provide and explain standard or reference cost data relevant to the ‘project’ approach (e.g., license costs) or the ‘service’ approach (for the required service area and location) in a strictly bilateral and confidential manner before the start of the actual tender process.

We would appreciate receiving your replies and the information you can provide us with at the latest on 28 February 2005. Can you please provide a cover letter in which the above points are answered and in which a summary list of the documentation is detailed?

Your replies and the resulting exchange of information with you will be treated as commercial in confidence by the Agency.

You will find in the Annexes the following information:

- Annex A: The ESA IT environment
• Annex B: DoCeP overview
• Annex C: Procurement strategy
• Annex D: Legal environment
• Annex E: Questions and concerns

Thank you for your collaboration and we look forward to hearing from you,

Best regards,

[Signature]

Palle Soerensen
Head of the Information System Integration Division

Cover note and documentation should be sent (preferably in PDF format) to:

E-mail: jurgen.scholz@esa.int

Alternatively as hardcopy via surface mail to:

Mr Jürgen Scholz
ESA/ESRIN
Via Galileo Galilei
00044 Frascati (Rome)
Italy

Phone +39-06-94180-434

—

Disclaimer

• The Agency is free to use the information provided by the potential bidders only within the scope of the preparation of the planned Invitation to tender preparation.

• In no case the information provided by the potential bidders will be considered for the evaluation and selection of the winning bid. The evaluation and selection will be performed only in bidders proposals based upon the issue of a formal ESA Invitation to Tender.
This Request for Information and the information provided by the potential bidders do not bind the Agency in any way to place a contract.

**Annex A – The ESA IT Environment**

This section should provide some additional information, which might be relevant for the preparation of the answer to the RFI and the planned tender.

The **Department and its Objectives**

The ESA Information Systems Department is responsible for the provision of corporate business applications and information services, and the informatics hardware and basic software in line with established strategic guidelines.

The Information Systems Department is a service organisation in support of ESA objectives; it provides in general end-to-end services encompassing an Information System, its maintenance and its operation services, enabling ESA activities to be performed by ESA staff.

The Information Systems Department is ISO9001-certified.

**Infrastructure Outsourcing**

- Currently, ESA’s IS infrastructure is operated via a service contract.

- ESA’s IS infrastructure will be completely outsourced (tender to be issued in the medium term): Delegation of provision, monitoring, management and coordination of the IS services and their sustaining & operations engineering and user support processes

- Relevant infrastructure elements:
  - Lotus Notes – e-mail
  - SmartStream – financial system
  - SharePoint – collaboration environment
  - DAM (user database, single sign-on, authentication services; LDAP)

**User locations**

**Internal:**

- Four main establishments: ESA HQ – Paris (France); ESTEC – Noordwijk (Netherlands); ESRIN – Frascati (Italy); ESOC – Darmstadt (Germany)
Smaller sites in Europe, US, and Russia

External: All ESA member states.

Current contracts

- Datamat: Informs-2, ODMS.
- Sapienza: “Science DMS” instances and services.
Annex B – DoCeP Overview

Global Objectives DoCeP – Mission Statement

This project shall, in a planned time frame of about three years,

- Implement a document-centric portal, integrating the following functions and services:
  - Content and document management (compound document handling, search and retrieval, library services including version control, document-level security; check-in/check-out),
  - Collaboration (including authoring, capturing, and re-use of information),
  - Reporting and information distribution (pull & push),
  - Enterprise-level workflow (forms, review/approval processes, change management) and business process management,
  - Security (access control, digital signatures, enterprise digital rights management), and
  - Archival and records management.
- Integrate a ‘Collaboration Environment’ for workgroups as well as a ‘Smart Enterprise Suite’ (which will also be the foundation for the DoCeP concept) for large corporate user groups targeting mainly Directorate and Programme¹ needs for document management

Context

The Information Systems Department strives to ensure that content and document management become an important part of the Agency’s business infrastructure. Most of the information that exists in ESA is unstructured, and there is an ever-growing imperative to manage this unstructured content. Content and document management (CM/DM) software provide business-enabling technologies that the Information Systems should offer to internal customers to gain strategic competitive advantage.

CM/DM consultancy services and end user assistance (Helpdesk and document acquisition support) in concert with a solid CM/DM strategy and product/service offering will make it possible to arrive at a critical mass that will allow to run such services in an efficient and cost-effective manner.

Current Situation

¹ The Agency is composed of a number of Directorates (e.g., Launchers, Science, Resources, …) under the governance of the ESA Director General. Directorates carry out programmes or projects (such as the construction of a satellite).
The Agency’s document management infrastructure currently comprises the following elements:

- **Informs-2.** This application, which is still in use for DODIS (the ‘official Document Distribution System’)\(^2\), ESALEX (‘ESA Legal Texts’), and a few other DM systems, has reached the end of its lifetime. While, at the end of the 1990s, this system was running in more than 20 instances (i.e., it had a critical mass of customers) its outdated architecture today is difficult and costly to maintain.

- **Lotus Notes document libraries.** Currently the only ‘operational’ DM offering of the ESA Information Systems Department, widely distributed and in use, but without formal control and guidelines for utilization.

- **The ‘Science DMS’,** a custom-developed Oracle database with some DM capabilities. Widely distributed, well performing application with strong service support.

- **Some smaller DM services (ODMS – the DODIS data entry front-end, Rocade) are still maintained, but should be replaced in the near future.**

\(^2\) This application – see also Figure 1 – provides access to the Agency’s official documents via the so-called ‘Calendar of meetings’, where users obtain the list of documents to be discussed during an upcoming meeting with the possibility to download these; via a search facility; via a document order basket; via a push distribution of documents by e-mail. The Agency is governed by a number of so-called ‘delegate bodies’ (e.g., the Council, the ‘Administrative and Finance Committee’ – AFC, etc), whose members are the national delegates.
Figure 1 DODIS welcome screen

In addition, the ESA Information Systems Department has gained extensive knowledge and customer confidence in the domain of web content management (i.e., the automated management of complex and large web sites versus the classical ‘document management’ system) with its involvement in the ESA Communications Portal (ESA-CP) project.

Needs

A pilot working group is currently analyzing Microsoft SharePoint as offering for a ‘Collaboration Environment’\(^3\), i.e., a workgroup document management and collaboration suite (which is competing with domino.doc, QuickPlace and SameTime in the ‘low end’ DM market).

Bearing in mind that ESA programmes (e.g., Launchers) and Directorates (e.g., D/OPS) require CM/DM capabilities and ODMS/DODIS\(^4\) need to be replaced and extended (e.g., known need for Records Management), an action to gain an overview on the CM/DM market and evaluate ECM/SES systems has been

\(^3\) The ‘Collaboration environment’ is not part of this RFI; whatever solution is chosen (e.g., SharePoint) will be integrated into the DoCeP concept at some stage in the future.

\(^4\) Need expressed by customer based on Internal Audit report.
initiated. The ECM/SES suite may evolve into a document-centric portal offering in
order to cater for enhanced security requirements (including tight access control,
document level security, digital signatures and enterprise digital rights
management) and the document management requirements originating from an
organization-wide ISO 9000 certification. In this domain, the project could offer –
beside a technical solution and expertise – consultancy services for ISO DM
requirements.

In the context of the ESA-CP, the ESA Information Systems Department has
recently started a project to offer generic (external) web hosting services.

Synergies with the DAM project (directory, access authorization, role management
and single sign-on services based on Novell eDirectory, iChain, and SecureLogin),
PUMA (delegates directory) and possible benefits for other business applications
(like DM services for the Project Management initiative) shall be noted.

Document-Centric Portal Implementation

Starting from the ‘e-Council and Programme Board [eCPB] Portal’
(OEMS/DODIS replacement with extensions), the ‘Document-Centric Portal’ (see
Fig. 2) will evolve into the entry point for all (document-dependent) applications.
The implementation shall be phased as follows.

Phase 1: eCPB Preparation Cycle

The eCPB preparation cycle will be the first “instance” of an ECM/SES
implementation comprising the document planning and preparation workflow for
official documents, collaborative authoring (including document templates for
official documents), review and approval cycles, and the translation workflow. The
“Follow-up workflow” will record the status of documents and resulting actions
following the meeting in which the document was discussed. This will, for instance,
allow locating all “documents in force” (legal texts) and will be the first step in
replacing ESALEX as well.

All content of ODMS will be migrated and ESA-internal access is granted to Admin
and Info notes, as well as Vacancy Notes. Authorized users will be granted access
to original documents as well as restricted official documents.

The number of users in this phase is estimated to be around 50 (all internal).

---

5 DG requirement
6 The official source for Admin and Info notes, as well as VNs is ODMS.
7 These documents are currently made available via ODMS Web to the Translations Division.
ODMS Web could be abandoned at this stage.
Phase 2: eCPB Delegates Portal

At the end of Phase 1, the eCPB Portal will already contain all official documents of interest to delegations.

The suite is now to be extended to become a real ‘Delegates Portal’, which besides replacing DODIS, shall offer the possibility to reduce or abolish the distribution on paper of official documents; it shall as well cater for the implementation of enhanced security and access control features (via the access control and directory layer - SSO including role management, via DAM).

By providing a different “view” on the eCPB content (legal texts only), a new version of ESALEX could be released for possibly different user group as well.

The number of users in this phase is estimated to be around 2000 internal and 500 external.

Phase 3: Records Management
Following eCPB Phase 1, the document-centric Portal shall be extended with Records Management (RM) capabilities. Conceptually, a common cross-application document workflow and storage layer should achieve this, in order to make the RM module available to other DM instances as well.

Thus, official documents and other official records will be archived in a way compliant with international standards and statutory obligations of ESA.

**Phase 4: Programme/Directorate Portals**

Programme or Directorate Portals can be built upon concepts inherited from the e-Council Portal, and extended with local ‘flavours’, for instance:

- Web publication (web content management)
- Project change management workflow
  - E.g., Engineering Change Requests
- Correspondence management and follow-up
- ISO-certification-related procedures
  - E.g., project approval workflow

The (conceptual) integration of the e-mail system for document distribution as well as e-mail archival is an additional important build block.

The number of internal users increases to a maximum of about 4000 (all ESA staff and on-site contractors) and 1000 external.

**Phase 5: Integration**

The Storage/DM layer as well as the cross-application enterprise document workflow layer shall make available standard interfaces to allow corporate applications to make use of the DM services (e.g., Project Management initiative). The ‘document-centric’ portal may at this stage develop into an application integration portal, which besides providing access to all corporate applications also supports their integration.

Once a number of ECM/SES instances have been rolled out, a cross-repository accessibility layer shall be added to this Portal. This layer will implement some ‘knowledge management’ elements such as providing retrieval access to all (document) repositories, especially legacy DM applications.

SharePoint (tbc) services will complement the Document-centric Portal offering with workgroup collaboration and (low end) DM features. These services shall interface “outward-bound” with other elements of the DoCeP; e.g., a document
created in the Collaboration Environment is routed to a Directorate Portal or the RM module.

Services

The Document-Centric Portal offering must be complemented with at least the following services:

- Consultancy on CM/DM for/to end users (e.g., ‘local’ DM strategies and specific working procedures; application of DM/RM policies in the ‘real world’)
- End user support:
  - Training
  - CM/DM Helpdesk
  - Documentalists (document acquisition and related services)
Annex C - Procurement Strategy

The Agency is currently discussing two different procurement strategies, one being the classical ‘project approach’ and one being the entire outsourcing of the project and its operations to a service provider.

A complete DM/CM solution typically consists of:

- Use of the commercial off-the-shelf system (“license”)
- Parametrisation / customization of the system (“project”)
- Delivery of the service (“service”)

ESA is considering two procurement strategies for this project:

In the “project approach” ESA acquires a “turn-key” solution and operates it on its own infrastructure. The services are acquired separately.

In the “service approach” ESA acquires system functionality and related services on a monthly basis, regulated by a Service Level Agreement. The infrastructure and the document base are typically (but not necessarily) off-site.

For the DoCeP project, ESA has a preference for the service approach but may still revert to the project approach. In both cases, it expects a Contractor, or a consortium led by a Prime Contractor, to be entirely responsible for the full delivery of the solution / provision of the service.

ESA has a policy to avoid custom development on top of off-the-shelf systems. Ideally the software part of the solution should be obtained via a mere parameterisation (not modification or bespoke extension) of the COTS. If any modification / customisation of the COTS is necessary to meet the requirements, it should be kept to the bare minimum.

Project Approach

In this scenario, the prime contractor would at least be responsible for:

- Choice of the ECM/SES suite and procurement of licenses
- Phased implementation of the project
- Support to the installation and operations at ESA premises and on ESA infrastructure
- Training of system administrators
- Training of first line Helpdesk staff
- Training of end users
o Provision of second line support
o Provision of other services:
  o DM/CM consultancy (optional)
  o Document acquisition (“documentalists”)
  o Bulk scanning (optional)
  o External storage of paper documents (optional)

Service Approach

In this scenario, the prime contractor would at least be responsible for:

o Phased provision of the services required by the Agency. In this case, the choice of the ECM/SES suite, the procurement of the licenses, and the implementation should be ‘transparent’ to the Agency. The prime contractor would also be responsible for the hosting and operations of the service.
o Training of first line Helpdesk staff
o Training of end users
o Provision of second line support
o Provision of other services:
  o DM/CM consultancy
  o Document acquisition (“documentalists”)
  o Bulk scanning (optional)
  o External storage of paper documents (optional)

Additional Information

o The tender might initially be limited to Phase 1 (or Phase 1, 2 and 3 with elements of 5), with the remaining phases to be quoted as options depending on the success of the implementation/service delivery and the interest of internal customers.
o While the tender evaluation criteria have not been defined yet, a good combination of product choice/vendor, implementation and service delivery is an asset.
Annex D – The Legal Environment

The European Space Agency is Europe’s gateway to space. Its mission is to shape the development of Europe’s space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe.

ESA has been created by a convention in 1975 (see www.esa.int, ‘About ESA’ for more information).

This section contains legal/institutional requirements that may apply to the project:

- Legal status of the ESA archives
- ESA Security Regulations

Legal Status of ESA Archives

The ESA convention grants a status of inviolability to the archives of the Agency - see http://esamultimedia.esa.int/docs/SP1271En_final.pdf:

“Article III. The archives of the Agency shall be inviolable.

...

Article IV. The Agency shall have immunity from jurisdiction and execution [...] The Agency's property and assets, wherever situated, shall be immune from any form of requisition, confiscation, expropriation and sequestration. They shall also be immune from any form of administrative or provisional judicial constraint, ...

...

Article X. The circulation of publications and other information material sent by or to the Agency shall not be restricted in any way.”

ESA Security Regulations (from ESA/C/R/CLXI/Res. 1 (Final))

“2. ESA Security has the following principal objectives:

(a) to safeguard ESA classified information from espionage, compromise or unauthorised disclosure;
(b) to safeguard ESA classified information handled in communications and information systems and networks, against threats to its integrity and availability;
(c) to safeguard installations housing ESA classified information from sabotage and malicious wilful damage;
(d) in the event of failure, to assess the damage caused, limit its consequences and adopt the necessary remedial measures.

...

5. Levels of classification

Information is classified at the following levels:

ESA TOP SECRET (ESA TS): this classification shall be applied only to information and material the unauthorised disclosure of which could cause exceptionally grave prejudice to the essential interests of ESA and/or of one or more of its Member States.

ESA SECRET (ESA S): this classification shall be applied only to information and material the unauthorised disclosure of which could seriously harm the essential interests of ESA and/or of one or more of its Member States.

ESA CONFIDENTIAL (ESA C): this classification shall be applied to information and material the unauthorised disclosure of which could harm the essential interests of ESA and/or of one or more of its Member States.

ESA RESTRICTED (ESA R): this classification shall be applied to information and material the unauthorised disclosure of which could be disadvantageous to the interests of ESA and/or of one or more of its Member States.

...

8. The security measures shall:
(a) extend to all persons having access to ESA classified information, classified information-carrying media, all premises containing such information and important installations;
(b) be designed to detect persons whose position might endanger the security of classified information and important installations housing ESA classified information and provide for their exclusion or removal;
(c) prevent any unauthorised person from having access to ESA classified information or to installations which contain it;
(d) ensure that ESA classified information is disseminated solely on the basis of the need-to-know principle which is fundamental to all aspects of security;
(e) ensure the integrity (i.e. prevention of corruption or unauthorised alteration or unauthorised deletion) and the availability (i.e. access is not denied to those needing and authorised to have access) of all ESA classified information, and especially of such information stored, processed or transmitted in electromagnetic form.

...
INFORMATION SECURITY (INFOSEC)
System Security Principles and Procedures

38. All communications, information systems and networks (hereinafter SYSTEMS) handling ESA classified information require security measures to protect the confidentiality, integrity and availability of that information. The security measures to be applied to those systems will be determined by the appropriate Security Accreditation Authority (SAA) and will be commensurate with the assessed risk and consistent with the policy stated in the ESA Security Regulations.

39. A balanced set of security measures shall be identified and implemented to create a secure environment in which a SYSTEM operates. The fields of application of those measures concern physical elements, personnel, non-technical procedures, computer and communications operating procedures.

40. All SYSTEMS handling information classified ESA CONFIDENTIAL and above shall be accredited.

41. There shall be a Security Accreditation Authority (SAA) responsible for ensuring the compliance of SYSTEMS with the ESA Security Regulations.

42. For SYSTEMS belonging to ESA, the SAA shall be:

- for a SYSTEM used by ESA headquarters, establishments and facilities:
  • if the SYSTEM is not connected with a national information system and does not use or process national classified information, the accreditation process is an internal process;
  • otherwise, a panel staffed by ESA and the appropriate NSA/DSA (of Member States concerned by interconnection or national classification) conducts the accreditation process and validates accreditation statements.

- for SYSTEMS used by national bodies or contractors, the NSA/DSA of the Member State where the SYSTEM is deployed. In such a case the NSA/DSA conducts the accreditation process and validates accreditation statements.

43. For all SYSTEMS handling information classified ESA CONFIDENTIAL and above, a SYSTEM-Specific Security Requirement Statement (SSRS) shall be approved by the SAA.

44. Users of the SYSTEM shall be cleared and have a need-to-know, as appropriate for the classification and content of the information handled within their particular SYSTEM. Access to certain equipment (e.g. cryptographic) or information specific to security of SYSTEMS will require a special clearance issued by the relevant NSA/DSA.

COUNTER-SABOTAGE AND OTHER FORMS OF MALICIOUS WILFUL DAMAGE
45. Physical precautions for the protection of important installations housing classified information are the best protective security safeguards against sabotage and malicious wilful damage, and clearance of personnel alone is not an effective substitute.

INDUSTRIAL SECURITY
46. All entities participating in industrial activities, which involve access to information classified ESA CONFIDENTIAL and above must hold a Facility Security Clearance (FSC).

... 48. The prime contractor shall be contractually required, under penalty of termination of their contract, to take all measures prescribed by ESA and/or NSAs/DSAs respectively for safeguarding all ESA classified information generated by or entrusted to the contractor, or embodied in articles manufactured by the contractor.

..."
Annex E – Open Questions

DoCeP concept and services

1. Do you have experience with the proposed breakdown/phasing? How are the answers to this question affected a gradual increment of the user population?
2. What is the range of DM services offered by your company (e.g., training, documentalists, bulk scanning, off site paper archives, ...)?
3. Do you offer expert advise/consultancy on CM/DM (e.g., support for the design of the RM filing plan, etc.)? How can these services be deployed?
4. Which other DM services are offered?
5. How could the DM services evolve in the lifetime of the project?
6. ECM/SES suite chosen:
   - What ECM/SES (off-the-shelf product) would you base your offer upon? Please explain your choice.
   - Outline product evolution.
   - How flexible / easy to parameterise is the selected product, ie is it possible to adapt to the customer’s requirements without programming / customising?
   - In your experience with past projects based on this product, how much parameterisation and how much customisation has been necessary?
   - How is the adaptation carried forward to new releases of the COTS?

Procurement strategy

7. Is your company in a position to deliver the solution required either in a service approach or in a project approach?
8. ‘Project’ approach: Please outline possible broad timeline (for all phases), more detailed schedule (for phases 1 – 3), effort (phases 1 - 3), cost/payment profile options (s/w licenses) and exit clauses.
9. ‘Service’ approach: Please outline broad timeline (all phases), more detailed schedule (for phases 1 – 3), payment profile options (renting of s/w licenses?) and exit clauses.
   - SLA for service delivery (service metrics) – can you provide an example?
   - In this approach, what would be your cost structure / cost model? In particular:
     a. How is the licence cost distributed over time?
     b. How is the project cost distributed over time?
     c. What is the break-even point between the service approach and the project approach?
   - What is the typical duration of a contract under this approach?
• What is the typical portion of the solution which becomes the property of the customer:
  a. Intellectual Property (eg screen layouts)
  b. Project implementation (ie actual code)
  c. COTS licences
  d. etc.

10. Which advantages/disadvantages do you see for both approaches? Does the service vs. project approach influence timeline or schedule?

ESA IT environment and legal requirements

11. Would you be in a position to provide on-site service to all four major ESA establishments under a single management?

12. Explain how you would cater for the security requirements listed in this document for both procurement approaches (to which extend is your solution capable of supporting our security requirements?). If possible, name clients, which have similar requirements.

13. The ESA convention grants a status of inviolability to the archives of the Agency; this in turn might impose constraints on the legal status of the location where information is stored and might turn out to be incompatible with locating the archives with a service provider. What is your position on this matter?
  o In a ‘service’ approach, what would be the physical location of the on-line and off-line document archives? Would you accommodate a request to have the physical archives in a specific ESA location?

14. Explain the prerequisites to be provided by ESA:
  • Classical project approach: Hardware and software infrastructure, ....
  • Service approach: network connectivity; integration with ESA infrastructure, ...