OPEN CALL FOR TENDERS

Tender Specifications

"Provision of consultancy services: Identity Management, Electronic Authentication and Secure Development"

ENISA P/06/10/TCD

LOT 1 - Management of multiple identities

LOT 2 - Mapping of Security Services to Authentication Levels

LOT 3 - Secure Software Engineering

Part 1 Introduction

Part 2 Technical Description

Part 3 Administrative Details

Annex I	Legal Entity Form
Annex II	Financial Identification Form
Annex III	Declaration of Honour for exclusion criteria & absence of conflict of interest
Annex IV	Financial Offer form
Annex V	Draft Service contract
Annex VI	Declaration by Authorised Representative
Annex VII	Consortium Form
Annex VIII	Sub-Contractors Form

CONTENTS

PART 1 INTRODUCTION

1. BACKGROUND

Communication networks and information systems have become an essential factor in economic and social development. Computing and networking are now becoming ubiquitous utilities in the same way as electricity or water supply. The security of communication networks and information systems, in particular their availability, is therefore of increasing concern to society. This stems from the possibility of problems in key information systems, due to system complexity, accidents, mistakes and attacks to the physical infrastructures which deliver services critical to the well-being of European citizens.

For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises, and public sector organisations within the European Union (EU), thus contributing to the smooth functioning of the Internal Market, a European Network and Information Security Agency (ENISA) was established on 10 March 2004[1].

2. SCOPE

The Agency shall assist the European Commission and EU Member States, and in consequence cooperate with the business community, in order to help them to meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market, including those set out in present and future Community legislation, such as in the Directive 2002/21/EC.

3. OBJECTIVES

The Agency's objectives are as follows:

- The Agency shall enhance the capability of the Community, EU Member States and, as a consequence, the business community to prevent, to address, and to respond to network and information security problems.
- The Agency shall provide assistance and deliver advice to the Commission and EU Member States on issues related to network and information security falling within its competencies as set out in the Regulation.
- Building on national and Community efforts, the Agency shall develop a high level of expertise.
- The Agency shall use this expertise to stimulate broad cooperation between actors from the public and private sectors.
- The Agency shall assist the Commission, where called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security.

[1] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. A "European Community agency" is a body set up by the EU to carry out a very specific technical, scientific or management task within the "Community domain" ("first pillar") of the EU. These agencies are not provided for in the Treaties. Instead, each one is set up by an individual piece of legislation that specifies the task of that particular agency.

4. TASKS

In order to ensure the fulfilment of its objectives, the Agency's tasks will mainly be focused on:

- Advising and assisting the Commission and the Member States on network and information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks.
- Promoting risk assessment and risk management methods to enhance our capability to deal with network and information security threats.
- Awareness raising and cooperation between different actors in the network and information security field, notably by developing public-private partnerships in this field.

The Agency shall base its operations on carrying out a work programme adopted in accordance to the relevant Articles of the establishing regulation. The work programme does not prevent the Agency from taking up unforeseen activities that follow its scope and objectives and within the given budget limitations.

5. ORGANISATIONAL FRAMEWORK

The bodies of the Agency comprise a Management Board, an Executive Director (and his staff) and a Permanent Stakeholder Group. The Executive Director is responsible for managing the Agency and performs his/her duties independently.

The Management Board is entrusted with the necessary powers to: establish the budget, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the Agency, approve the Agency's work programme, adopt its own rules of procedure and the Agency's internal rules of operation, appoint and remove the Executive Director. The Management Board should ensure that the Agency carries out its tasks under conditions which enable it to serve in accordance with the Regulation establishing it.

The Permanent Stakeholders Group is composed of experts representing the relevant stakeholders, such as Information and Communication Technologies industry, consumer groups and academic experts in network and information security. The Permanent Stakeholders Group advises the Executive Director in the performance of his duties under the Regulation, in drawing up a proposal for the Agency's work programme and in ensuring communication with the relevant stakeholders on all issues related to the work programme.

The Executive Director will establish, in consultation with the Permanent Stakeholders Group, ad hoc Working Groups composed of experts Where established, the ad hoc Working Groups shall address in particular technical and scientific matters.

6. ADDITIONAL INFORMATION

Further information about ENISA can be obtained on its website: www.enisa.europa.eu.

For ENISA's legal base please click here.

PART 2 TECHNICAL DESCRIPTION

1. LOT 1: MANAGEMENT OF MULTIPLE IDENTITIES

1.1 CONTEXT

The development and deployment of electronic identity management (eIDM) solutions in European electronic applications stands at a crossroads. Over the past decade, European Member States and EEA countries have gradually rolled out identity management solutions that were best suited to their national goals and ambitions. The goals of such initiatives were uniformly the same: improving administrative efficiency, improving accessibility and user-friendliness, and above all, the reduction of costs. At the European level, these goals could be advanced by improving the interoperability of electronic identification/authentication solutions being offered at the national level.

With the advent of the Internet each person has the opportunity of living two lives in parallel in the real as well as in the virtual world. A trend observed over the last few years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet.

An area of particular interest is the management of multiple identities. In this context, “identity” is being considered in a broad sense (i.e. eID, Federated identity, RFID, avatars, etc.). Possible application environments for investigation are virtual on-line worlds where the notions of anonymity, pseudonymity, unlinkability and unobservability should be explored.

1.2 OBJECTIVES AND TASKS

The report shall identify and describe the ways of management of multiple identities, and provide best practices and guidelines for different audiences.

More specifically, the objective of this tender shall be achieved through the following tasks:

- Identify and describe a broad set of types of identities
- Identify and describe general techniques of managing multiple identities
- Identify good practices and develop key guidelines for three communities:
    - Technical – software developers, standards development organisations
    - Policy – policy makers
    - End users – organisations leading awareness raising campaigns

The requirements for achievement of above tasks should include:

- Making reference to existing studies related to identity management
- Considering “identities” in a broad sense, i.e. eIDs, Federated identities, RFIDs, avatars etc.
- Grouping identities in classes (including for example online games, social networks, banking, e-government etc.)
- Taking into account the issues of:
    - Unlinkability of different identities
    - Security of credentials
    - Use of the same credentials for managing different identities
    - Role of anonymity

- Taking into account efforts in this area undertaken on the European level
- Presenting findings in a form of different scenarios and including case studies
- Proposing possible standardisation activities in this area

1.3 EXPECTED SKILLS

The performance of the above mentioned activities requires professionals that have good professional multi disciplinary knowledge on all or a large subset of the following fields:

- Good knowledge of the area of identity management;
- Good knowledge of relevant security areas;
- Proven inside knowledge and experience of European initiatives in the field of electronic identity, identity management, authentication mechanisms and interoperability of authentication systems;
- Experience in writing reports on technical issues to a non-technical audience;
- English as working language;
- Excellent communication skills;
- Excellent Project Management skills.

1.4 LIST OF DELIVERABLES

The final report should identify and describe the ways of management of multiple identities, and providing best practices and guidelines. Specific parts of the report are:

D1 – Table of contents (skeleton of the final report)

D2 – State of the art (description of types of identities and classification)

D3 – Methods of management of multiple identities

D4 – Identification of scenarios and case studies

D5 – Guidelines for three communities (Technical, Policy and End users)

D6 – Final report

English is the language to be used for all the documents (interim and final reports, project management reports etc) produced

1.5 DURATION OF THE SERVICE

The Tenderer is required to make a proposal in their tender for the time schedule of the activities in order to carry out the project (e.g. including a Gantt chart). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this Call for Tenders. As an estimation, we expect this to be in the order of 50 - 60 person days.

The Tenderer should cooperate with relevant ENISA experts through the whole process of the preparation of the report.

The specific parts of the report should be delivered following the deadlines below:

D1, D2 – 17th September 2010

D3, D4 – 8th October 2010

D5, D6 – 29th October 2010

After each deadline ENISA will have one calendar week to provide its comments. The contractor will be required to respond to these comments within the next calendar week and fully process them within two weeks (i.e. the comments for D1 and D2 should be presented by ENISA before the 24th September, the contractor should present the plan of accommodating them before 1st October and fully process them before the 8th October).

Please note that the above mentioned dates cannot be changed.

1.6 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The contractor is required to be present at ENISA premises for all necessary meetings and for collecting all relevant information to conduct the analysis. For this purpose network based collaborative tools (i.e. videoconferencing) could also be used.

At least the following communication with the contractor is expected.

- One kick off meeting organised either at ENISA premises, or at the contractors premises or alternatively at a location convenient to both.
- Regular teleconferences on the progress achieved (at least one per 2-3 weeks)

It should be mentioned that the costs of such business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings.

Quality assurance, review and final approval of deliverable, and project sign-off will take place at a location to be agreed on later. Informal and regular contacts should be maintained by telephone and e-mail.

1.7 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **50,000.00 Euros** (fifty thousand Euros) covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises, use of conferencing equipment, telephone calls, etc.).

2. LOT 2: MAPPING OF SECURITY SERVICES TO AUTHENTICATION LEVELS

2.1 CONTEXT

The development and deployment of electronic identity management (eIDM) solutions in European electronic applications stands at a crossroads. Over the past decade, European Member States have gradually rolled out identity management solutions that were best suited to their national goals and ambitions. The goals of such initiatives were uniformly the same: improving administrative efficiency, improving accessibility and user-friendliness, and above all, the reduction of cost. At European level, these goals could be advanced by improving the interoperability of eID solutions being offered at the national level. However, security issues are a major obstacle to the development of European-wide authentication schemes.

Since 2007, ENISA has published a number of reports on security issues relating to eID applications[1].

One of the more important European initiatives in the area of eIDM is the STORK project:

"*The aim of the STORK project is to establish a European eID Interoperability Platform that will allow citizens to establish new e-relations across borders, just by presenting their national eID. Cross-border user authentication for such e-relations will be applied and tested by the project by means of five pilot projects that will use existing government services in EU Member States. In time however, additional service providers will also become connected to the platform thereby increasing the number of cross-border services available to European users*"[2].

Future eIDM initiatives will need to examine, on the basis of the results of the STORK project, how the pilot infrastructure can be expanded into a full-scale system. This will entail the identification of the assumptions that had to be made in the course of the project and the creation of suitable and acceptable solutions to replace these assumptions. Based on currently available information, further efforts will be needed to ensure the trustworthiness and reliability of the infrastructure, by eliminating any remaining security weaknesses and by implementing a suitable legal framework within the Member States[3]. In order to support these activities and objectives, ENISA is commissioning this report.

2.2 OBJECTIVES AND TASKS

The purpose of this tender is to appoint a Contractor to produce a report on security services[4] required for cross-border electronic authentication in Europe.
An authentication mechanism is a technique designed to allow one party to gain assurance that the identity of another is as declared. The means used can vary from a simple combination of username and password to a smart card using cryptography.
The STORK project has defined several security levels[5] for electronic authentication, so-called QAA levels. A QAA level reflects the strength of the mechanism. An application or a service might

[1] ENISA website, Electronic Identity (eID), http://www.enisa.europa.eu/act/it/eid/
[2] STORK website, http://www.eid-stork.eu/
[3] ENISA, Report on the state of pan-European eIDM initiatives, http://www.enisa.europa.eu/act/it/eid/eidm-report
[4] We refer to "security services" as defined in: Web Services Glossary, W3C Working Group Note 11 February 2004, http://www.w3.org/TR/ws-gloss/. A typical security services is, for example, an electronic authentication based on a private-public key pair where the private key is stored on a smart card and protected by a PIN.

require a certain security level for its authentication mechanisms. At the same time, an application might require a maximum complexity for authentication, thereby reducing the number of appropriate authentication levels.

The Contractor will review the authentication levels and the mapping of security services to these authentication levels as defined by STORK and provide an expert opinion. The Contractor shall explicitly take into account authentication mechanisms deployed in European countries that do not participate in the STORK project. If necessary, the Contractor shall propose useful amendments and/or corrections. The target audience for the report shall be policy decision-makers and industry professionals. Technical details should be provided in the Annexes of the report.

The Contractor will be required to work together with a team of ENISA experts ("ENISA team") as well as individual external experts (“the external experts”) who have either volunteered or are being compensated by ENISA for this project. The report shall be based on the preliminary findings of the ENISA team and the external experts which will be provided to the Contractor before the kick-off of the activity. Draft versions of the report shall be sent to the ENISA team and to the external experts on a regular basis and comments shall be taken into account. The Contractor is expected to steer the discussions with the other participants. This should be done via efficient use of remote communication tools such as web and telephone conferencing or email.
Concerning the publication of the report, please note article I.9.1., "Assignment of Ownership", of the contract specifications.

2.3 EXPECTED SKILLS

- Experience in writing reports on technical issues for a non-technical audience
- Expert knowledge about European initiatives in relevant areas, such as electronic authentication, identity management or electronic identity cards
- Understanding of policy issues related to electronic identity (eID) at national and European level
- Experience in IT security
- English as a working language
- Excellent communication skills
- Excellent project management skills

2.4 LIST OF DELIVERABLES

The following deliverable shall be delivered by the contractor:

- White Paper on: “Mapping of Security Services to Authentication Levels”.

Specific requirements:

- Shall be compliant with the objectives given in the section "Objectives and Tasks"

[5] STORK Materials, D2.1 - Framework Mapping of Technical/Organisational Issues to a Quality Scheme, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=579

- The readability and presentation of the report are very important; graphics and diagrams should be used where effective
- Any quoted *or paraphrased* work should be explicitly referenced; the originality of the report will be verified
- The report should reference existing documents in this area
- The report should show evidence of having consulted a representative sample of experts
- The report shall be written in English
- The final report shall be self-contained and self-explanatory; it shall contain an executive summary
- The final report and all draft versions must be delivered in one of the following file formats: **.doc** (Microsoft Word 2003), .**docx** (Microsoft Word, latest version), or **.odt** (Open Office)

Further details will be defined between ENISA and the successful contractor.

2.5 DURATION OF THE SERVICE

The Tenderer is required to make a proposal for the time schedule of the activities in order to carry out the project (e.g. a Gantt chart). In its offer the Tenderer should indicate the estimated amount of person days required to accomplish all tasks associated with this lot. As an estimation, we expect this to be in the order of 50 - 60 person days.
This service contract is provisionally scheduled to be awarded around start of July 2010. The draft report should be finalised and presented to ENISA not later than three months after this date.

2.6 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The contractor is required to be present for all necessary meetings and for collecting all relevant information to conduct the risk assessment. For this purpose network-based collaborative tools (e.g. videoconferencing) can also be used. Informal and regular contacts should be maintained by telephone and e-mail.

All project management should be done through electronic or telecommunication means. During the whole process of assessment, regular contacts with the ENISA team shall be maintained. It is important to note that if face-to-face meetings (especially the kick-off meeting), are necessary, all expenses will be covered by ENISA outside of this contract. Please do not provision for any expenses in this regard.

2.7 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget **cannot exceed €50,000 Euros** (fifty thousand Euros) covering all tasks executed and including all costs.

3. LOT 3 – SECURE SOFTWARE ENGINEERING

3.1 CONTEXT

The Secure Services Programme

Many of the NIS issues with most impact on ENISA's stakeholders are rooted in application-layer vulnerabilities. Therefore, ENISA wishes to adopt an end-to-end approach addressing all system layers and process steps. Important examples of application risks with a high negative impact are:

- Malware vectors used to launch DDoS attacks including those on Estonia and Georgia. Malware can also lead to criminal activities, such as click-fraud, spam or spyware.
- Cloud computing risks.
- Risks to applications supporting supply chains
- Risks to dependable systems software including SCADA applications.

In order to address risks to the application layer, ENISA launched a programme of activities focusing on this area. It is considered particularly important to focus on developing reliable information on the level of risk from different types of application vulnerabilities, since any remedial action should be based on objective data.

The goals of the secure applications and services programme are

1. To support the development of reliable sources of data about the nature, distribution and severity of current application-related security incidents and risks (threats and vulnerabilities).
2. Based on priorities derived from the information collected in point 1: to identify, support and *where necessary* initiate forums**,** methodologies, reference architectures, secure development programmes, educational programmes and principles focused on addressing application risks.
3. To support the development of reliable assurance mechanisms for applications.

In all cases an approach considering legal, policy, technical and educational perspectives should be used.

3.2 OBJECTIVES AND TASKS

Secure Software Engineering

Within the secure services programme, one of the key objectives is to reduce the risks arising from insecure software engineering (development, deployment and maintenance practices). Since a lot of initiatives already exist in this area, ENISA intends to work closely with existing secure software engineering initiatives, to collect and aggregate information, and to support, foster and promote such existing efforts. New initiative(s) would be proposed only where it is determined that there is no existing work in an area of secure software engineering.

Driven by the priorities of ENISA's stakeholders, ENISA will collect, aggregate, support, enhance and promote best practices. The activity will focus on specific areas of software engineering, including:

- Requirements engineering
- Procurement criteria for secure software
- Risk based development
- Security in agile methods
- Policy frameworks for web access control.
- Security testing methodologies and code reviewing
- Patch and update management

ENISA will neither duplicate work done by existing programmes and initiatives in the area of secure software engineering, nor favour any one programme above another. Instead, it needs to profit from its independent position, its strong background in risk analysis and best practice development and its stakeholder network to add value to existing initiatives in the most effective and impartial way.

The first step in the context of this activity will be to take stock of what existing initiatives exist, across the software engineering lifecycle among industry stakeholders and in terms of government led programmes, e.g. OWASP, NESSI, CLASP, SANS, SAFECODE, MS SDL, etc. The stock-taking exercise will be used to analyze the differences and similarities between the identified secure software engineering programmes and look at how these initiatives and related good/best practices relate to different market actors (users/customer and providers/developers, private and public organizations, etc) and how they are incorporated in procurement guidelines both for government and industry tenders (or if there are any initiatives aiming specifically at secure software engineering guidelines for procurement processes). The study will take into account both global initiatives and any national or international initiatives operating within Europe.

Using the results of the stock-taking, and an analysis of the software engineering risk landscape, the contractor will make recommendations on how ENISA should position itself, in order to maximize its impact on minimizing risks arising from software engineering weaknesses.

The project is organized into three tasks. Their requirements are given below.

3.2.1 Task 1 – Stock-Taking

Making use of:

- Its network of contacts among relevant stakeholders
- Contacts to stakeholders provided by ENISA
- Appropriate desktop research
- Direct contact with stakeholders and organisations via telephone or email, where appropriate.

the contractor will take stock of the following *types of secure software engineering initiatives*:

- Industry consortia
- Government policy initiatives
- Academic initiatives

- Initiatives involving all of the above

The report should cover initiatives including, but not limited to, the following *areas of software engineering* (proposals should be made for further areas):

- Requirements engineering
- Procurement criteria for secure software
- Risk based development
- Security in agile methods
- Policy frameworks for web access control.
- Security testing methodologies and code reviewing
- Patch and update management

The report should cover initiatives including, but not limited to, the following *types of software applications*:

- Web applications
- Mobile and smartphone applications
- Desktop applications
- Supply chain applications
- Highly dependable applications (e.g. SCADA).
- Financial applications

The report should NOT cover:

- Military software
- Software supporting the layer 4 (the transport layer) and below of the ISO/ITU OSI model.

3.2.2 Task 2 – Analysis, Good Practices and Recommendations

The report should begin by presenting in no more than 5 pages, an overview of the areas of secure software engineering in which contributions from ENISA might have impact.

The contractor will present the results of Task 1 in a clearly written report where the various initiatives can be easily compared. In particular, the report should present, for each initiative:

- A description of the contribution of the initiative to the overall area of secure software engineering.
- A qualitative description of the approach taken.
- A summary of the stakeholders involved.
- Application areas covered (e.g. web software, high assurance software).
- Areas of software engineering covered (e.g. requirements engineering).
- Contact details of the organisation.
- International coverage.
- Key reports and documents (regular and one-off).
- Liaisons and connections to other organisations.
- Details and recommendations of how ENISA could potentially support or join the organisation, if recommended.

Based on this information, and knowledge of the domain of secure software engineering, the contractor will propose a strategy for ENISA to impact secure software engineering which:

- Maximises impact:
    - Leverages ENISA's existing expertise, best practice development processes, while taking into account the resources ENISA is able to commit to this activity (this will be discussed with the contractor).
    - Leverages existing initiatives without duplicating effort.
    - Leverages ENISA's independent positioning.
    - Takes into account the impact of various risks addressed (i.e. the strategy should prioritise the mitigation of the highest impact risks).
- Is impartial – does not favour any single initiative or organisation (while still selecting collaboration with initiatives which can achieve maximum impact). Furthermore, it should not propose any further third party contracts as part of the strategy.
- Focuses on maximising results within Europe, without ignoring the need to collaborate globally in order to achieve European results.

The report should clearly specify traceable sources for all information and well-reasoned argumentation for any judgements made. The report should clearly separate conclusions from any technical argumentation supporting them.

3.2.3 Task 3 – Project Management

The main objective of this task is to define and implement appropriate management mechanisms, sound planning and resource allocation according to proven expertise and prior knowledge of the subject.

As part of this task the contractor should also provide justification for subcontracting if required, interact with ENISA staff and external experts, and provide regular management reporting. This will ensure the punctual delivery of good quality results of this study within the budget allocated.

The prospective contractor is expected to submit to the Agency detailed Gantt Charts and accompanying documentation with sufficient details including:

- Scheduling of all tasks and activities within the tasks,
- Identification of milestones and critical activities,
- Assignment of experts and person days to tasks and activities
- Identification of possible risks and suggestions to mitigate them
- Quality assurance and peer review measures to ensure high quality results
- Detailed information on the expertise of the contractors on the tasks and topics of this tender including references to previous, relevant projects,
- Detailed CVs of experts proposed to be involved in all the tasks of the project
- Detailed justification for subcontracting tasks or parts of them. In that case, ENISA requires additional information on the
    - Tasks undertaken by the sub-contractor,
    - Expertise of the contractor and its experts,
    - Resources allocated to him/her
    - Co-ordination mechanisms among the prime and the sub contractors
    - Risk management method in case of delayed and/or low quality delivery of sub-contractor's outcomes

- Official statement of overall responsibility for the whole project and its results by the prime contractor

Based on the Gantt chart, the contractor is expected to deliver the following documents regularly:

- Brief monthly progress report on current activities (as they are defined in the Gantt chart), information on the progress achieved, next steps, possible risks affecting project, risk mitigation measures
- Early warning reports, at any time, if emerging risks threaten key milestones of the project and when the Agency needs to either be informed or take a decision.
- Teleconferences with ENISA staff every 2 weeks on the progress of the project and its tasks./

3.3 EXPECTED SKILLS

The performance of the abovementioned activities requires professionals that have good academic and professional multi disciplinary knowledge and experience of all or a sub set of the following fields:

- Proven professional and/or academic experience of secure software engineering at national and/or international level.
- Good experience in organising stock taking exercises, analysis skills, and creating strategy documents and recommendations on relevant subjects.
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements;
- Good professional experience in relevant security issues and disciplines (e.g. defence in depth, access control systems, requirements engineering, testing methodologies);
- Knowledge of ENISA, its role and its stakeholders
- Excellent project management skills including quality assurance
- Very good communication skills.

3.4 LIST OF DELIVERABLES

The following deliverables/outputs are required from the prospective contractor:

- Task 1 - Stock Taking – Delivery date August 15th 2010
- Task 2 - Analysis, Recommendations - Delivery date 30th September 2010
- Final Report – Secure software engineering, stocktaking and strategy recommendations for ENISA - Delivery date 30th September
- Professional Power Point presentation on the Final Deliverable - Delivery date 30th September

3.5 DURATION OF THE SERVICE

The Tenderer is required to make a proposal for the time schedule of the activities in order to carry out the project (e.g. a Gantt chart). In its offer the Tenderer should indicate the estimated amount

of person days required to accomplish all tasks associated with this lot. As an estimation, we expect this to be in the order of 40 person days.

The duration of this work is foreseen between April 2009 and September 2010.
More specifically:

- Task 1 should start by July 1st and finish not later than August 15th 2010
- Tasks 2 should start by August 15th 2010 and finish not later than end of September 2010
- Tasks 3 should start by July 1st 2009 and finish not later than end of September 2010

3.6 PLACE OF EXECUTION OF THE ACTIVITIES AND COMMUNICATIONS

The execution of the activities will take place at the Contractor's premises. The contractor is required to be present for all necessary meetings and for collecting all relevant information to conduct the risk assessment. For this purpose network-based collaborative tools (e.g. videoconferencing) can also be used. Informal and regular contacts should be maintained by telephone and e-mail.

All project management should be done through electronic or telecommunication means. During the whole process of assessment, regular contacts with the ENISA team shall be maintained. ENISA expects that the prospective contractor will perform, in the context of this study, the following business trip:

- Kick off meeting: either at the contractor premises, at ENISA's or at a place jointly decided by ENISA and the contractor

It should be mentioned that the costs of such business trips should be included in the total offer. ENISA will not additionally reimburse the contractor for taking part in these meetings.

Prior to the kick off meeting, the prospective contractor is expected to submit detailed Gantt charts and relevant documentation. These will be negotiated with ENISA and be confirmed as final.

3.7 TENDER RESULT AND ESTIMATED CONTRACT VALUE

The result of the evaluation of tenders will be the awarding of a Service Contract. The total estimated budget cannot exceed **30,000.00 Euros** (fifty thousand Euros) covering all tasks executed and including all costs (e.g. travelling expenses of the contractor to and from ENISA's premises, use of conferencing equipment, telephone calls, etc.).

The following articles apply to ALL LOTS:

[LOT 1, LOT 2 and LOT 3]:

4. CONTENT AND PRESENTATION OF THE TECHNICAL OFFER

The Tenderer shall enclose with the **Technical Offer** all documents and information that will enable its offer to be assessed in terms of quality and of compliance with the Specifications. An Offer shall include a description of the operational means and procedures to be implemented to perform the Contract, supported where appropriate by related documents.

An Offer shall cover the following aspects:

Description of the deliverables

The deliverables must be presented as requested in the section entitled “Deliverables”.

Management of provision of services

Project Management: a detailed description of the project management method to be used including quality assurance is required.

5. PRICE

Prices submitted in response to this Open Call for Tenders must be inclusive of all costs involved in the performance of the contract. Prices shall be submitted only in EUR and VAT excluded.

6. PRICE REVISION

Prices submitted in response to this Open Call for Tenders shall be fixed and not subject to revision.

7. COSTS INVOLVED IN PREPARING AND SUBMITTING A PROPOSAL

ENISA will not reimburse any costs incurred in the preparation and submission of a proposal. Any such costs must be paid by the Contractor.

8. PERIOD OF VALIDITY OF THE TENDER

Contractors must enclose a confirmation that the prices given are valid for 90 (ninety) days from the date of submission of the proposal.

9. PROTOCOL ON PRIVILEGIES AND IMMUNITIES OF THE EUROPEAN COMMUNITIES

ENISA is exempt from all taxes and duties, including value added tax (VAT), pursuant to the provisions of Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Contractors must therefore give prices which are exclusive of any taxes and duties and must indicate the amount of VAT separately.

10. PAYMENT ARRANGEMENTS

Payments under the Service Contract shall be carried out subject to prior approval of the Services by ENISA within 30 (thirty) days after an invoice is submitted to ENISA. One single payment will be made after receipt and approval of the deliverables by ENISA. An invoice must specify the specific deliverables covered. A note that accompanies the final deliverable must present the resources used for the deliverable presented. Time sheets should be submitted as appropriate.

11. CONTRACTUAL DETAILS

The result of the evaluation of tenders will be the awarding of one Service Contract for each LOT. If the same tenderer is successful for two or more LOTs then a consolidated contract may be awarded. A model of the Service Contract is proposed to the successful candidates (Annex V).

Please note *that the general conditions of our standard service contract cannot be modified. Submission of a tender by a potential contractor implies acceptance of this contract and all of the terms and conditions contained therein. It is strongly recommended that you have this draft contract checked and passed by your legal section before committing to submitting an offer.*

PART 3 ADMINISTRATIVE DETAILS

1. FORMAL REQUIREMENTS

1.1 Address and deadline for submission of the Tender:

You are invited to tender for this project and requested to submit your tender no later than **10 May 2010** either by:

a) **Registered post or express courier**. The postal service's dated stamp or the courier company's printed delivery slip and stamp will constitute proof of compliance with the deadline given above:

or

b) **Hand-delivery** (direct or through any authorised representative of the Tenderer) by 17.00 hours on **10 May 2010** in order to establish proof of the date of deposit, the depositor will receive from an official at the below-mentioned address, a receipt which will be signed by both parties, dated and time stamped.

Please note that in this case it is the date and time actually received at the ENISA premises that will count.

The offer must be sent to one of the following addresses:

Postal Address		Express Courier & Hand Delivery
European Network and Information Security Agency (ENISA) For the attention of: The Procurement Officer PO Box 1309 71001 Heraklion Greece	or	European Network and Information Security Agency (ENISA) For the attention of Procurement Section Science and Technology Park of Crete (ITE) Vassilika Vouton 700 13 Heraklion Greece

Please note that late despatch will lead to exclusion from the award procedure for this Contract.

1.2 Presentation of the Offer and Packaging

The offer (consisting of one original and two copies) should be enclosed in two envelopes, both of which should be sealed. If self-adhesive envelopes are used, they should be further sealed with adhesive tape, upon which the Tenderer's signature must appear.

The **outer envelope**, in addition to the above-mentioned ENISA address, should be marked as follows:

OPEN CALL FOR TENDER NO. **ENISA P/06/10/TCD**

"Provision of consultancy services: Secure Development, Identity Management and Electronic Authentication"

NOT TO BE OPENED BY THE MESSENGER/COURIER SERVICE

NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE **20th MAY 2010**
TENDERED BY THE FIRM: *<PLEASE INSERT NAME OF THE TENDERER/COMPANY>*

The **inner envelope** should also be similarly marked:

OPEN CALL FOR TENDER NO. **ENISA P/06/10/TCD**

"Provision of consultancy services: Secure Development, Identity Management and Electronic Authentication"

NOT TO BE OPENED BY THE OPENING COMMITTEE BEFORE **20th MAY 2010**
TENDERED BY THE FIRM: *<PLEASE INSERT NAME OF THE TENDERER/COMPANY>*

1.3 Identification of the Tenderer

Tenderers are required to complete the **Legal Entity Form (Annex I)** which must be signed by a representative of the Tenderer authorised to sign contracts with third parties. There is one form for 'individuals', one for 'private entities' and one for 'public entities'. A standard form is provided for each category - please choose whichever is applicable. In addition to the above, a **Financial Identification Form** must be filled in and signed by an authorised representative of the Tenderer and his/her bank (or a copy of the bank account statement instead of bank's signature). A specimen form is provided in **Annex II**. Finally a **Declaration by Authorised Representative (Annex VI)** must also be completed for internal administrative purposes.

The **Legal Entity Form** must be supported by the following documents relating to each Tenderer in order to show its name, address and official registration number:

a) For private entities:

- A legible copy of the instrument of incorporation or constitution, and a copy of the statutes, if they are contained in a separate instrument, or a copy of the notices of such constitution or incorporation published in the national or other official journal, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the above paragraph have been amended, a legible copy of the most recent amendment to the instruments mentioned in the previous indent, including that involving any transfer of the registered office of the legal entity, or a copy of the notice published in the relevant national or other official journal of such amendment, if the legislation which applies to the Tenderer requires such publication.
- If the instruments mentioned in the first paragraph have not been amended since incorporation and the Tenderer's registered office has not been transferred since then, a written confirmation, signed by an authorised representative of the Tenderer, that there has been no such amendment or transfer.
- A legible copy of the notice of appointment of the persons authorised to represent the Tenderer in dealings with third parties and in legal proceedings, or a copy of the publication of such appointment if the legislation which applies to the legal entity concerned requires such publication.
- If the above documents do not show the registration number, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

b) For Individuals:

- A legible copy of their identity card or passport.
- Where applicable, a proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or any other official document showing the registration number.
- If the above documents do not show the VAT number, a copy of the VAT registration document, where applicable.

c) For Public Entities:

- A copy of the resolution decree, law, or decision establishing the entity in question or failing that, any other official document attesting to the establishment of the entity.

All tenderers must provide their Legal Entity Form (Annex I) as well as the evidence mentioned above.

In case of a joint bid, only the co-ordinator must return the Financial Identification form (Annex II).

The Tenderer must be clearly identified, and where the Tender is submitted by an organisation, a company the following administrative information and documents must be provided (see administrative identification form attached as Annex I:
Full name of organisation/company, copy of legal status, registration number, address, person to contact, person authorised to sign on behalf of the organisation (copy of the official mandate must be produced), telephone number, facsimile number, VAT number, banking details: bank name, account name and number, branch address, sort code, IBAN and SWIFT address of bank: a bank identification form must be filled in and signed by an authorised representative of each Tenderer and his banker.

Tenders must be submitted individually. If two or more applicants submit a joint bid, one must be designated as the lead Contractor and agent responsible.

1.4 Participation of consortia

Consortia, may submit a tender on condition that it complies with the rules of competition. The 'Consortium Form' (Annex VII) must be completed and submitted with your offer.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific tender procedure. Such a grouping (or consortia) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender. All members of a consortium (i.e., the leader and all other members) are jointly and severally liable to the Contracting Authority.

In addition, each member of the consortium must provide the required evidence for the exclusion and selection criteria (*Articles 2 and 3 below*). Concerning the selection criteria "technical and professional capacity", the evidence provided by each member of the consortium will be checked to ensure that the consortium as a whole fulfils the criteria.

The participation of an ineligible person will result in the automatic exclusion of that person. In particular, if that ineligible person belongs to a consortium, the whole consortium will be excluded.

1.5 Subcontracting

In well justified cases and subject to approval by ENISA, a contractor may subcontract parts of the services. The 'Sub-contractors Form' (Annex VIII) must be completed and submitted with your offer.

Contractors must state in their offers what parts of the work, if any, they intend to subcontract, and to what extent (% of the total contract value), specifying the names, addresses and legal status of the subcontractors.

The sub-contractor must not sub-contract further.

Sub-contractors must satisfy the eligibility criteria applicable to the award of the contract. If the identity of the intended sub-contractor(s) is already known at the time of submitting the tender, all sub-contractors must provide the required evidence for the exclusion and selection criteria.

If the identity of the sub-contractor is not known at the time of submitting the tender, the tenderer who is awarded the contract will have to seek ENISA's prior written authorisation before entering into a sub-contract.

Where no sub-contractor is given, the work will be assumed to be carried out directly by the bidder.

1.4 Signatures of the Tender

Both the technical and the financial offer must be signed by the Tenderer's authorised representative or representatives (preferably in blue ink).

1.5 Total fixed price

A total fixed price expressed in Euro must be included in the Tender. The contract prices shall be firm and not subject to revision.

1.6 Language

Offers shall be submitted in one of the official languages of the European Union (preferably in English).

1.7 Opening of the Tenders

The opening of received tenders will take place on **20th May 2010 at 10:00** at ENISA Building, Science and Technology Park of Crete, GR - 70013 Heraklion, Greece.

2. GROUNDS FOR EXCLUSION OF TENDERERS

2.1 Reasons for Exclusion

Pursuant to Article 29 of Council Directive 92/50/EC relating to Public Service Contracts and to Article 93 of the Financial Regulation, ENISA will exclude Tenderers from participation in the procurement procedure if:

They are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or

Are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

They have been convicted of an offence concerning their professional conduct by a judgement which has the force of res judicata;

They have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;

They have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

a. They have been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;

b. Following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations.

Tenderers must certify that they are not in one of the situations listed in sub-article 2.1 (see Annex III: Exclusion criteria and non-conflict of interest form). If the tender is proposed by a consortium this form must be submitted by each partner.

2.2 Other reasons for not awarding the Contract

Contracts may not be awarded to Candidates or Tenderers who, during the procurement procedure:

a. Are subject to a conflict of interest;

b. Are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the contract procedure or fail to supply this information;

c. Any attempt by a Tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or ENISA during the process of examining, clarifying, evaluating and comparing tenders will lead to the rejection of his offer and may result in administrative penalties.

See last paragraph point 2.1.

2.3 Confidentiality and Public Access to Documents

In the general implementation of its activities and for the processing of tendering procedures in particular, ENISA observes the following EU regulations:

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data;

- Regulation (EC) No. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.

3. SELECTION CRITERIA

The following criteria will be used to select the Tenderers. If the Tender is proposed by a consortium these criteria must be fulfilled by each partner.

Documentary evidence of the Tenderers' claims in respect of the below-mentioned criteria is required.

3.1 Professional Information

The Tenderer must provide evidence of enrolment (declaration or certificates) in one of the professional or trade registers, in country of establishment.

3.2 Financial and Economic Capacity

Proof of financial and economic standing may be furnished by one or more of the following references:

- Annual accounts, balance sheet or extracts there from where publication of the balance sheet is required under company law in the country of establishment;
- Statement of the undertaking's overall turnover and its turnover in respect of the services to which the contract relates for the previous three financial years.

If, for any valid reason, the service provider is unable to provide the references requested by the contracting authority, he may prove his economic and financial standing by any other document which the contracting authority considers appropriate.

3.3 Technical Background

The prospective contractor should provide evidence (e.g. CVs of experts, previous projects in this field, references from clients, etc.) of expertise and knowledge on the topics mentioned below:

3.3.1 For LOT 1 - Management of multiple identities

- Experience in the area of identity management;
- Experience in the relevant security areas;
- Proven inside knowledge and experience of European initiatives in the field of electronic identity, identity management, authentication mechanisms and interoperability of authentication systems;
- Experience in writing reports on technical issues to a non-technical audience;

3.3.2 For LOT 2 - Mapping of Security Services to Authentication Levels

- Expert knowledge about European initiatives in relevant areas, such as electronic authentication, identity management or electronic identity cards
- Experience in IT security technologies
- Understanding of policy issues related to electronic identity (eID) at national and European level
- Project management capabilities; proven delivery of projects on time and on budget; experience with projects of ambitious European scope

3.3.3 For LOT 3 - Secure Software Engineering

- Proven professional and/or academic experience of secure software engineering at national and/or international level.
- Good experience in organising stock taking exercises, analysis skills, and creating strategy documents and recommendations on relevant subjects.
- Excellent knowledge of data collection and validation methods including the ability to produce clear and understandable text equipped with graphical elements;
- Good professional experience in relevant security issues and disciplines (e.g. defence in depth, access control systems, requirements engineering, testing methodologies);
- Professional project management skills including quality assurance
- Very good communication skills.

4. AWARD CRITERIA

The following award criteria apply to LOTS 1, 2 and 3 identically:

4.1 Quality of the Offer

Once the Tenderer has demonstrated the appropriate capacity to perform the Contract on the grounds of the selection criteria, the offer will be assessed on the basis of the award criteria.

No	Qualitative award criteria		Weighting (max. points)
1.	**Technical compliance**	Compliance with the technical descriptions (part 2 of this document)	20/100
2.	**Quality and accuracy of content and structure**	Quality of the proposal and accuracy of the description to provide the requested services	30/100
3.	**Project Team**	Composition of project team (ratio senior/juniors), work flows and review cycles of the output, direct involvement of senior staff, and distributions of tasks amongst experts; quality reviews of deliverables.	30/100
4.	**Methodology**	Selected survey methodology and project management	20/100
Total Qualitative Points (QP)			**100**

Minimum attainment per criterion

Offers scoring less than 50% for any criterion will be deemed to be of insufficient quality and eliminated from further consideration.

Minimum attainment overall

Offers scoring less than 60% after the evaluation process will be considered to be of insufficient quality and eliminated from the following phase.

The sum of all criteria gives a total of 100 points. The respective weighting between the different awards criteria depends on the nature of the services required and is consequently closely related to the terms of reference. The award criteria are thus quantified parameters that the offer should comply with. The **qualitative award criteria** points will be weighted at **70%** in relation to the price.

4.2 Price of the Offer

Tenders must state a total fixed price in Euro. Prices quoted should be exclusive of all charges, taxes, dues including value added tax in accordance with Article 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities. Such charges may not therefore be included in the calculation of the price quoted.

ENISA, in conformity with the Protocol on the Privileges and Immunities of the European Community annexed to the Treaty of April 8th, 1965, is exempt from all VAT.

Offers exceeding the maximum price set in Part 2: **Article 1.7 for LOT 1, Article 2.7 for LOT 2 and Article 3.7 for LOT 3**, will be excluded. The cheapest offer will receive the maximum points and the rest of the candidate's offers will be awarded points in relation to the best offer as follows

$$P_P = (P_C / P_B) \times 100$$

where;

P_P = Weighted price points
P_C = Cheapest bid price received
P_B = Bid price being evaluated

5. AWARD OF THE CONTRACT

The contract will be awarded to the offer which is the most cost effective (offers the best value for money) which obtains the highest number of points after the final evaluation on the basis of the ratio between the **quality criteria (70%) and the price (30%).** The following formula will be used:

$$TWP = (Q_P \times 0.7) + (P_P \times 0.3)$$

where;

Q_P = Qualitative points
P_P = Weighted price points
TWP = Total weighted points score

6. PAYMENT AND STANDARD CONTRACT

Payments under the Service Contract shall be made in accordance with article I.5 of the Special Conditions and article II.4.3 of the General Conditions (see Annex V)

In drawing up their bid, the Tenderer should take into account the provisions of the standard contract which include the “General terms and conditions applicable to contracts”

7. VALIDITY

Period of validity of the Tender: 90 days from the closing date given above. The successful Tenderer must maintain its Offer for a further 220 days from the notification of the award.

8. LOTS

This Tender is divided into Lots.

- **LOT 1 - Management of multiple identities**
- **LOT 2 - Mapping of Security Services to Authentication Levels**
- **LOT 3 - Secure Software Engineering**

9. ADDITIONAL PROVISIONS

- Changes to tenders will be accepted only if they are received on or before the final date set for the receipt of tenders.
- Expenses incurred in respect of the preparation and presentation of tenders cannot be refunded.
- No information of any kind will be given on the state of progress with regard to the evaluation of tenders.
- All documents submitted by Tenderers will become property of ENISA and will be regarded as confidential.

10. NO OBLIGATION TO AWARD THE CONTRACT

Initiation of a tendering procedure imposes no obligation on ENISA to award the contract. Should the invitation to tender cover several items or lots, ENISA reserves the right to award a contract for only some of them. ENISA shall not be liable for any compensation with respect to Tenderers who’s Tenders have not been accepted. Nor shall it be so liable if it decides not to award the contract.

11. DRAFT CONTRACT

A Service Contract will be proposed to the selected candidate. A draft copy of which is included as Annex V to this tender.

12. SPECIFIC INFORMATION

12.1 Timetable

The timetable for this tender and the resulting contract(s) is as follows:

Title: **Provision of consultancy services:**
Secure Development, Identity Management and Electronic Authentication

ENISA P/06/10/TCD

Summary timetable comments

Launch of tender - Contract notice to the Official Journal of the European Union (OJEU)	**24 March 2010**	
Deadline for request of information from ENISA	**4 May 2010**	
Last date on which clarifications are issued by ENISA	**6 May 2010**	
Deadline for submission of offers	**10 May 2010**	in case of hand-delivery (05:00 pm local time. This deadline is fixed for the receipt of the tender in ENISA's premises)
Opening of offers	**20 May 2010**	At 10:00 Greek time
Date for evaluation of offers	**20 May 2010**	At 11:00 Greek time
Notification of award to the selected candidate	End May 2010	Estimated
Contract signature (following '14 day standstill' period)	Mid – late June 2010	Estimated
Commencement date of activities	End June/start July 2010	Estimated
Completion date of activities	October/November 2010	Estimated

CHECKLIST

WHAT MUST BE INCLUDED IN THE TENDER SUBMISSION:

PLEASE TICK EACH BOX ☐ AND **RETURN THIS CHECKLIST**

TOGETHER WITH YOUR OFFER

1. Technical Offer ☐
2. Legal Entity Form[7] (*Annex I*) *dated and signed* ☐
3. Financial Identification Form[8] *(Annex II*) *dated and signed* ☐
4. Declaration on Honour on exclusion criteria (*Annex III*) *dated and signed* ☐
5. Financial Offer (*Annex IV) dated and signed* ☐
6. Supporting documentation showing previous related experience as well as financial information and proof of registration ☐
7. Declaration by Authorised Representative (*Annex VI*) *dated and signed* ☐
8. Consortium form (*Annex VII) dated and signed - if applicable* ☐
9. Sub-Contractors form (*Annex VIII) dated and signed – if applicable* ☐

The tenderers' attention is drawn to the fact that any total or partial omission of documentation requested may lead the Contracting Authority to exclude the tender from the rest of the procedure.

[7] If you have provided a Legal Entity form to ENISA within the previous 6 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.

[8] If you have provided a Financial Identification form to ENISA within the previous 6 months maximum and no details have changed in the meantime, then you may provide a photocopy of this previous form.

ANNEX I

Legal Entity Form

The specific form, for either a;

c) public entity,

d) private entity or

e) individual entity,

is available for download in each of the 22 official languages at the following address: http://ec.europa.eu/budget/execution/legal_entities_en.htm

Please download the appropriate from, complete the details requested and include in your tender offer documentation.

ANNEX II

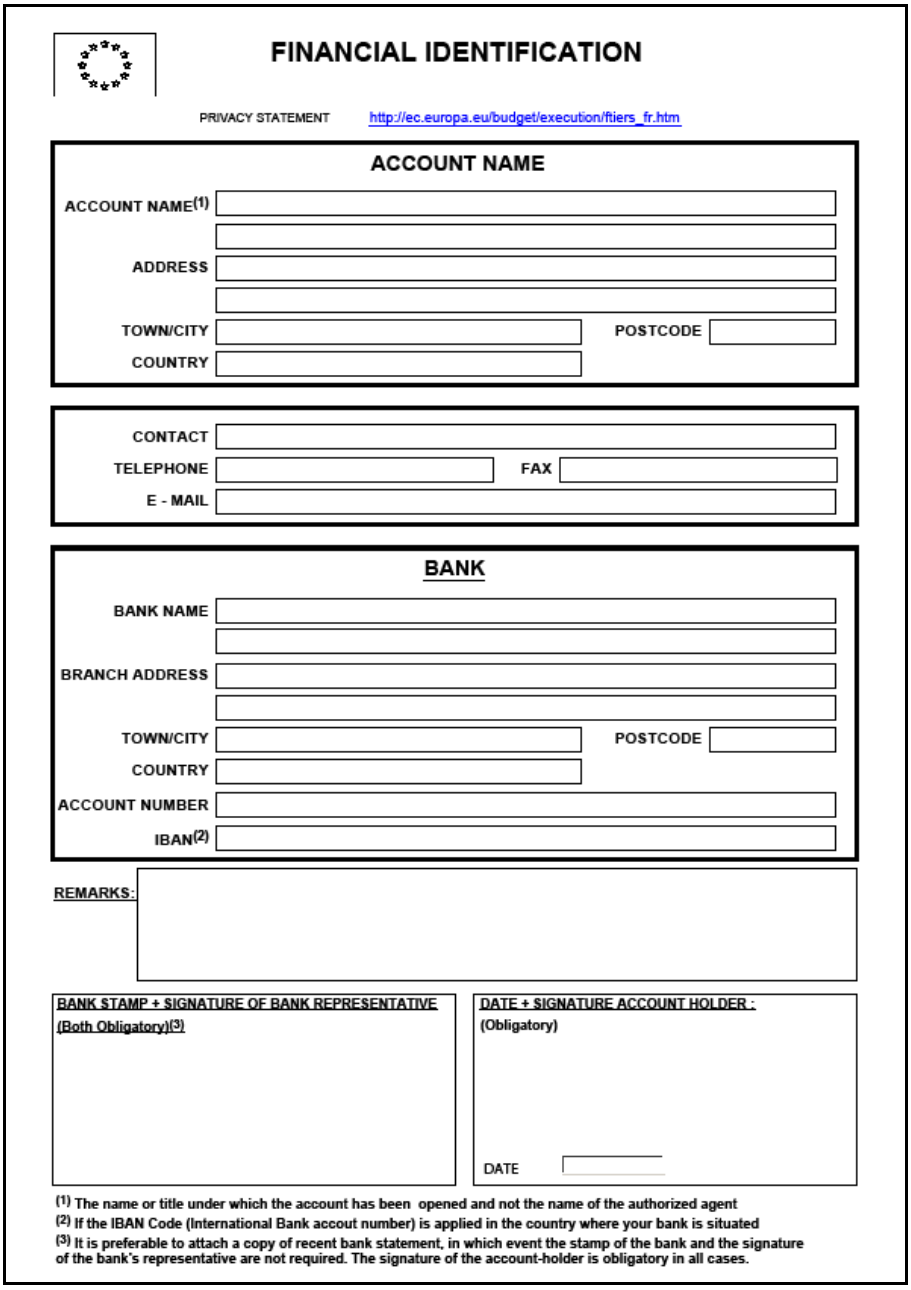
FINANCIAL IDENTIFICATION FORM

- SPECIMEN FOR THE TENDERER -

(to be completed by the Tenderer and his financial institution)

The Tenderer's attention is drawn to the fact that this document is a specimen, and a specific form in each of the 22 official languages is available for download at the following address:

http://ec.europa.eu/budget/execution/ftiers_en.htm



FINANCIAL IDENTIFICATION

PRIVACY STATEMENT http://ec.europa.eu/budget/execution/ftiers_fr.htm

ACCOUNT NAME

ACCOUNT NAME(1)

ADDRESS

TOWN/CITY POSTCODE

COUNTRY

CONTACT

TELEPHONE FAX

E - MAIL

BANK

BANK NAME

BRANCH ADDRESS

TOWN/CITY POSTCODE

COUNTRY

ACCOUNT NUMBER

IBAN(2)

REMARKS:

BANK STAMP + SIGNATURE OF BANK REPRESENTATIVE (Both Obligatory)(3)

DATE + SIGNATURE ACCOUNT HOLDER : (Obligatory)

DATE

(1) The name or title under which the account has been opened and not the name of the authorized agent
(2) If the IBAN Code (International Bank accout number) is applied in the country where your bank is situated
(3) It is preferable to attach a copy of recent bank statement, in which event the stamp of the bank and the signature of the bank's representative are not required. The signature of the account-holder is obligatory in all cases.

ANNEX III

DECLARATION OF HONOUR

WITH RESPECT TO THE

EXCLUSION CRITERIA AND ABSENCE OF CONFLICT OF INTEREST

The undersigned: …… *(Please print name)*

☐ in his/her own name *(if the economic operator is a natural person)*

or

☐ representing *(if the economic operator is a legal entity)*

Official name of the company/organisation: …….....…….

.....

Official legal form: .....

Official address in full: ..……

……...…….

……...…….

VAT (Tax) registration number:

……..……..…….

Declares that the company or organisation that he/she represents:

(a) is not bankrupt or being wound up, is not having its affairs administered by the courts, has not entered into an arrangement with creditors, has not suspended business activities, is not the subject of proceedings concerning those matters, and is not in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

(b) has not been convicted of an offence concerning professional conduct by a judgment which has the force of res judicata;

(c) has not been guilty of grave professional misconduct proven by any means which the contracting authorities can justify;

(d) has fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which it is established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

(e) has not been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;

(f) has not been declared to be in serious breach of contract for failure to comply with his contractual obligations subsequent to another procurement procedure or grant award procedure financed by the Community budget.

In addition, the undersigned declares on his honour:

(g) that on the date of submission of the tender, the company or organisation he represents and the staff proposed for this tender are not subject to a conflict of interests in the context of this invitation to tender; he undertakes to inform the ENISA Agency without delay of any change in this situation which might occur after the date of submission of the tender;

(h) that the information provided to the ENISA Agency within the context of this invitation to tender is accurate, truthful and complete.

By signing this form, the undersigned acknowledges that they have been acquainted with the administrative and financial penalties described under art 133 and 134 b of the Implementing Rules (Commission Regulation 2342/2002 of 23/12/02), which may be applied if any of the declarations or information provided prove to be false

.....	.....	.....
Full name	Signature	Date

ANNEX IV

FINANCIAL OFFER:

"Provision of consultancy services:
Secure Development, Identity Management and Electronic Authentication"

ENISA P/06/10/TCD

Please provide your financial lump sum offer for **any or all of** LOT 1, LOT 2 **or** LOT 3

LOT Description:	Number of 'Person days' required for completion of project.	**Your OFFER**
LOT 1 - Management of multiple identities *Please provide your lump sum price for the total deliverables.*	P/Days	**€**
LOT 2 - Mapping of Security Services to Authentication Levels *Please provide your lump sum price for the total deliverables*	P/Days	**€**
LOT 3 - Secure Software Engineering *Please provide your lump sum price for the total deliverables*	P/Days	**€**

Print name:	**Signature:**	**Date:**
(of the Tenderer or authorised representative)		

ANNEX V

Model Service Contract template

(See attached file)

ANNEX VI

DECLARATION BY THE AUTHORISED REPRESENTATIVE(S):

NAME OF LEGAL REPRESENTATIVE	
I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	
NAME OF 2nd LEGAL REPRESENTATIVE *(if applicable)*	
I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.	
First name	
Last name	
Title (e.g. Dr, Mr, Mrs)	
Position (e.g. Manager, Director)	
Telephone number	
Fax number	
e-mail address	
Website	

SIGNATURE: ……..……..…… **DATE:** .....

ANNEX VII – Consortium form

Name of tenderer:

Form of the Consortium: (Please cross the relevant box) [X]

Permanent: [ ] Legally established: [ ] Specifically for this tender: [ ]

	Name(s)	Address
Leader of the Consortium *(person authorised to conclude contract)*		
Partner 1*		
Partner 2*		

* add additional lines for partners if required. **Note that a subcontractor is not considered to be a partner.**

We confirm, as a partner in the consortium, that all partners are jointly and severally liable by law for the performance of the contract, that the leader is authorised to bind, and receive instructions for and on behalf of, each partner, that the performance of the contract, including payments, is the responsibility of the leader, and that all partners in the consortium are bound to remain in the consortia for the entire period of the contract's performance.

Signature: *Leader of consortium*	
Date:	
Signature: *Partner 1*	
Date:	
Signature: *Partner 2…etc*	
Date:	

ANNEX VIII – Sub-contractors form

	Name(s)	Address
Tenderer (person authorised to sign contract)		
Sub-contractor 1*		
Sub-contractor 2*		

* add additional lines for subcontractors if required.

As subcontractors for this tender, we confirm that we are willing to perform the tasks as specified in the tender documentation.

Signature: *Tenderer*	
Date:	
Signature: *Subcontractor 1*	
Date:	
Signature: *Subcontractor 2*	
Date:	