ANNEX I.B

IT hosting services for the Agency for the Cooperation of Energy Regulators

Framework Contract

CASE STUDY

OPEN CALL FOR TENDERS

ACER/OP/MMD/04/2016

Table of Contents

1. Introduction 3
2. The content of the case study 3
3. Description of the case study 4
3.1. Case study for a period of one (1) year 4
3.2. Case study for a period of two (2) years 9
3.3. Security applicable to points 3.1 and 3.2 above 14
3.4. Connectivity constraints applicable to points 3.1 and 3.2 above 14
4. Services to be provided by the tenderer applicable to points 3.1 and 3.2 above 15

1. Introduction

The tenderer shall submit a detailed proposal in writing on the basis of the case study presented below, under two assumptions:

- that the hosting services are provided to the Agency **for a period of one (1) year**;
- that the hosting services are provided to the Agency **for a period of two (2) years**.

The case study is a fictional exercise and does not commit the Agency to place such a request for service, should the tenderer be awarded the Framework Contract (hereinafter referred to as 'FWC').

2. The content of the case study

The tenderer's proposal for the case study shall include at least the following documents/information and the proposal should be limited to a maximum of 30 A4 pages:

a) a brief description of the approach the tenderer intends to adopt for the case study;

b) a description of the proposed hardware (type, model, brand, quantity, features, software provided);

c) a detailed description of how the housing (co-location) services for the equipment owned by the Agency are provided;

d) usage matrix containing each platform component and the role in the entire platform (e.g. Server X – Database Server);

e) a list of tasks to be completed by the proposed experts, and the utilisation of each single expert profile using the list of expert profiles as described by the Agency in the technical specifications. If a profile is missing in the Agency's list, the tenderer should add the proposed profile following the template of the Agency;

f) a detailed time schedule (i.e. GANTT chart) listing the tasks from the point above on a time line as well as the use of human resources per profile in terms of man days;

g) a proposal of Network Topology;

h) a proposal for technical and organisational security measures to be applied to the case study;

i) a proposal of the Service Level Agreement for the case study;

j) two (2) detailed financial proposals applicable to this case study as follows:

- a financial proposal for hosting services to be provided to the Agency **for a period of one (1) year** and
- a financial proposal for hosting services to be provided to the Agency **for a period of two (2) years**.

Both financial proposals shall be based on the tenderer's financial offer and/or the tenderer's detailed official price list.

IMPORTANT: The tenderer shall indicate where in the tenderer's financial offer and/or in the detailed official price list each proposed service/activity/etc. is specified. Both financial proposals shall be used to calculate the total reference price for the evaluation of the tenders as specified in Annex I tender specifications.

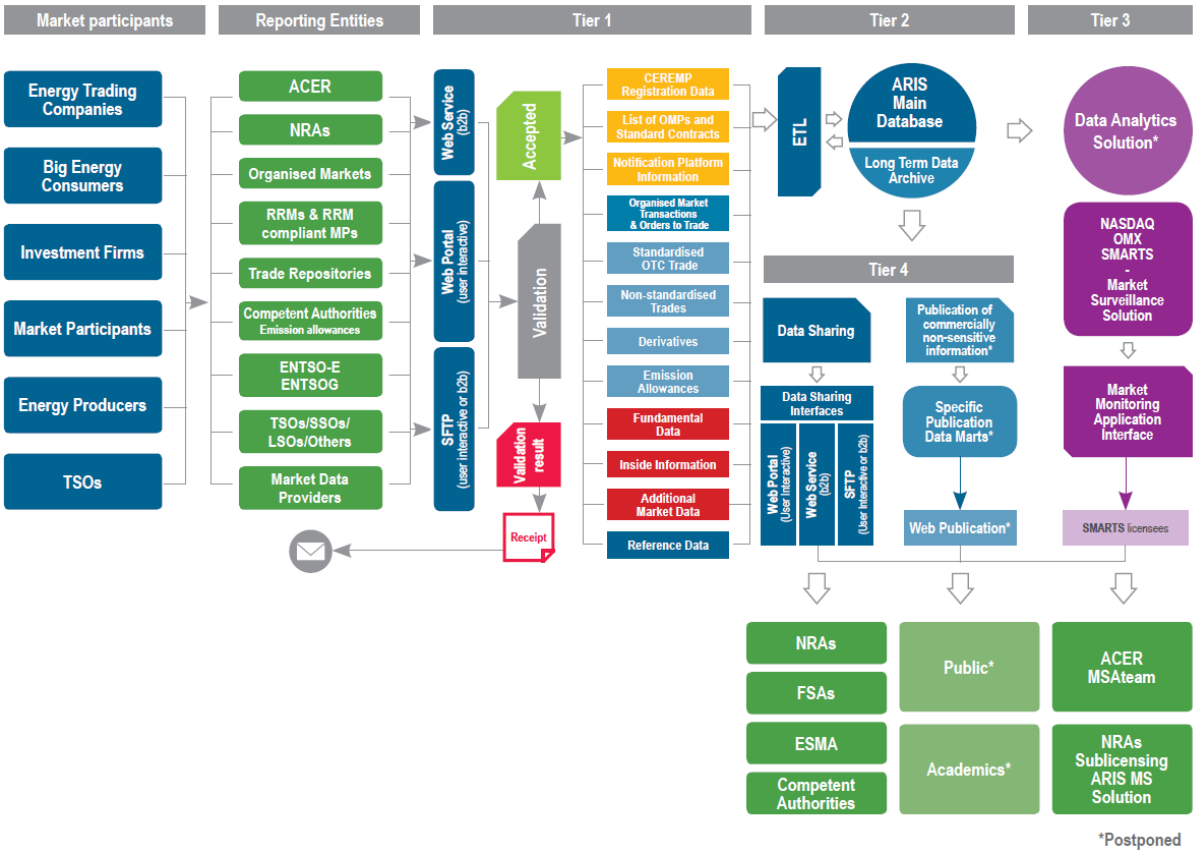
3. Description of the case study

3.1. Case study for a period of one (1) year

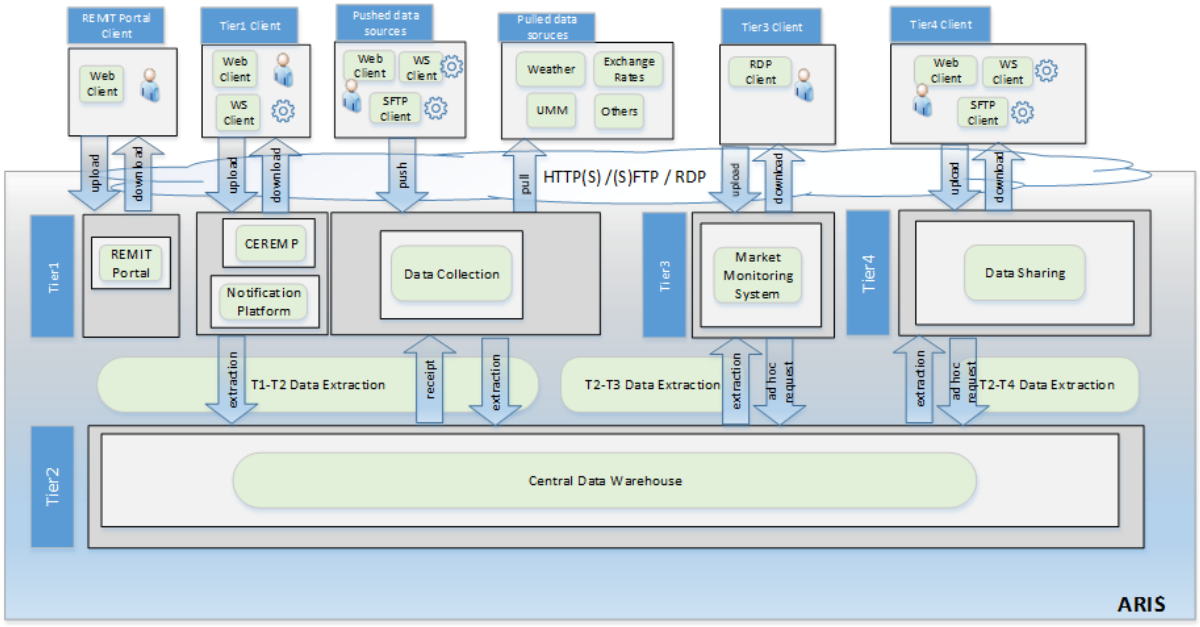
The Agency intends to launch a service request with the aim to cover the need to establish a working hosted system to host a Market Monitoring software platform which should serve twenty-eight (28) National Regulatory Authorities ('NRAs') and the Agency.

The Agency proprietary software will be designed as follows:

Functional view:



Technical view:



The estimations for capacity planning are:

Tier	Computing capacity	RAM capacity	Storage capacity	Storage performance
1	150 GHz	512 GB	5 TB	10.000 IOPS
2	150 GHz	512 GB	10 TB	20.000 IOPS
3	80 GHz	256 GB	10 TB	20.000 IOPS
4	115 GHz	100 GB	5 TB	10.000 IOPS

The list of key software architectural elements[1]:

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Tier 1: Web Server (**Registration, Collaboration, Administration**) web1, web2	2	2	4	100 GB	Apache HTTPD Server	HW LB (sticky session based on SSL Session ID)	Redundancy with 2 Apache servers

[1] If a specific Tier number is not provided for a component it may (but not necessarily has to) be placed in a separate zone (e.g. Tier 5).

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Tier 1: Web and SFTP Server (**Data Collection**) websftp3, websftp4, websftp5, websftp6	4	2	4	150 GB	Apache HTTPD and SFTP Server	HW LB (sticky session based on SSL Session ID only for web apps)	Redundancy with 4 Apache servers
Tier 4: Web and SFTP Server (**Data Sharing**) websftp7, websftp8	2	2	4	150 GB	Apache HTTPD and SFTP Server	HW LB (sticky session based on SSL Session ID only for web apps)	Redundancy with 2 Apache servers
Mail Server mail1, mail2	2	1	1	20 GB	Postfix for outgoing mail (SMTP)		Redundancy with 2 Mail servers
LDAP ldap1, ldap2	2	1	2	20 GB	Open LDAP Server	DNS LB	Redundancy with 2 LDAP servers with Master-Master replication
Authentication Server (**CAS**) cas1, cas2	2	1	4	20 GB	CAS (Central Authentication Service) deployed on Tomcat	HW LB	Redundancy with 2 CAS server in HA configuration
Tier 1: Application Server (**Registration**) app1, app2	2	4	12	100 GB /filestore1 (nfs)	CEREMP, CEREMPWS, NOTIFICATION PLATFORM, etc. deployed on Tomcat	HW LB	Redundancy with 2 application servers
Tier 1:	2	2	12	100 GB	ADMIN apps	HW LB	Web

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Application Server (**Collaboration, Administration**) app3, app4				/ filestore 1 (nfs)	deployed on Tomcat		applications: redundancy with 2 application servers
Tier 1: Application Server (**Data Collection**) app5, app6, app7, app8	4	2	12	100 GB / /filestore3 (nfs) /data (sshfs)	DCI, DCI-WS, DCI-SCHEDULER apps, etc. deployed on Tomcat	HW LB	Redundancy with 4 application servers
Tier 4: Application Server (**Data Sharing**) app9, app10	2	2	8	100 GB / /filestore4 (nfs) /data (sshfs)	Data sharing web app and ws etc. deployed on Tomcat	HW LB	Redundancy with 2 application servers
Tier 2: Application and SFTP Server (**Data extraction for T3**) app11, app12	2	2	8	100 GB / / filestore 4 (nfs)	Data extraction apps deployed on Tomcat and and sftp deamon	HW LB	Redundancy with 2 application servers
Log Management System app13, app14	2	2	4	20 GB / /filestore2 (nfs)	Log apps deployed on Tomcat	HW LB	Redundancy with 2 application servers
File Server(1) nfs1, nfs2	2	2	2	20 GB / /filestore1 (250 GB) /filestore2 (500 GB)	NFS Server		Active/Passive Heart beat configuration
File Server(2)	2	2	2	20 GB	NFS Server		Active/Passive Heart beat

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
nfs3, nfs4				/filestore3 (5 TB) /filestore4 (5 TB)			configuration
Terminal Servers	2	8	32	/ Windows O.S. (20GB)	Terminal Server	HW LB	Redundancy with 2 servers
Tier 3: Market Monitoring server	2	8	64	100 GB / Data (2TB)			Fail back server at the secondary site
Tier 2 Database Server (physical)	2	16	128	100 GB Data (2TB)	Oracle 12c R1 DBMS		Oracle RAC

The following additional requirements apply and must be present in the proposed solution:

- F6: 2 x 100 Mbps connection to the internet;
- F9: 1 x 1 Gbps connection between primary and secondary site;
- F11: 1 x 100 Mbps connection to the Agency;
- K1: 16 public IP addresses;
- K2: 3 domain names (.eu);
- K3: 16 DNS entries;
- I6: 1000 digital certificates from EU accredited CA;
- licensing (H) should be fully covered for OS and Hypervisors provided. No other licenses have to be included in the case study;
- a total of 600 man-days for the provision of services measured in man-days (G, I2 – I3, J2 – J4, L). For the purpose of this case study the total number of man-days should be evenly split between profiles (A, B and C) and for each profile 50 man-days should be provided on-site;
- a total of 1,000 requests to the service desk (J1).

For the purpose of this case study the tenderers are also required to consider how they would respond to the Agency's request to co-locate the following equipment without replicating to secondary site:

- C: 1 rack;
- E1: 4 standalone servers for co-location;
- E2: 1 storage controller for co-location;
- E3: 1 network connectivity device – switch for co-location;
- E4: 1 network security device – firewall for co-location;

- E5: 1 backup device for co-location.
- F2: 1 x 100 Mbps connection to Agency's premises
- F4: 1 x 10 Mbps connection to internet

The case study should provide the answers to the following questions:

1. How the infrastructure could be set up and managed?

2. Which type of IT experts should be included to set the system up and run it for a period of one (1) year?

3. How the security-related services (I1 – I7), licensing model (H) and support services (J1 – J4) and software related services (G) will be provided?

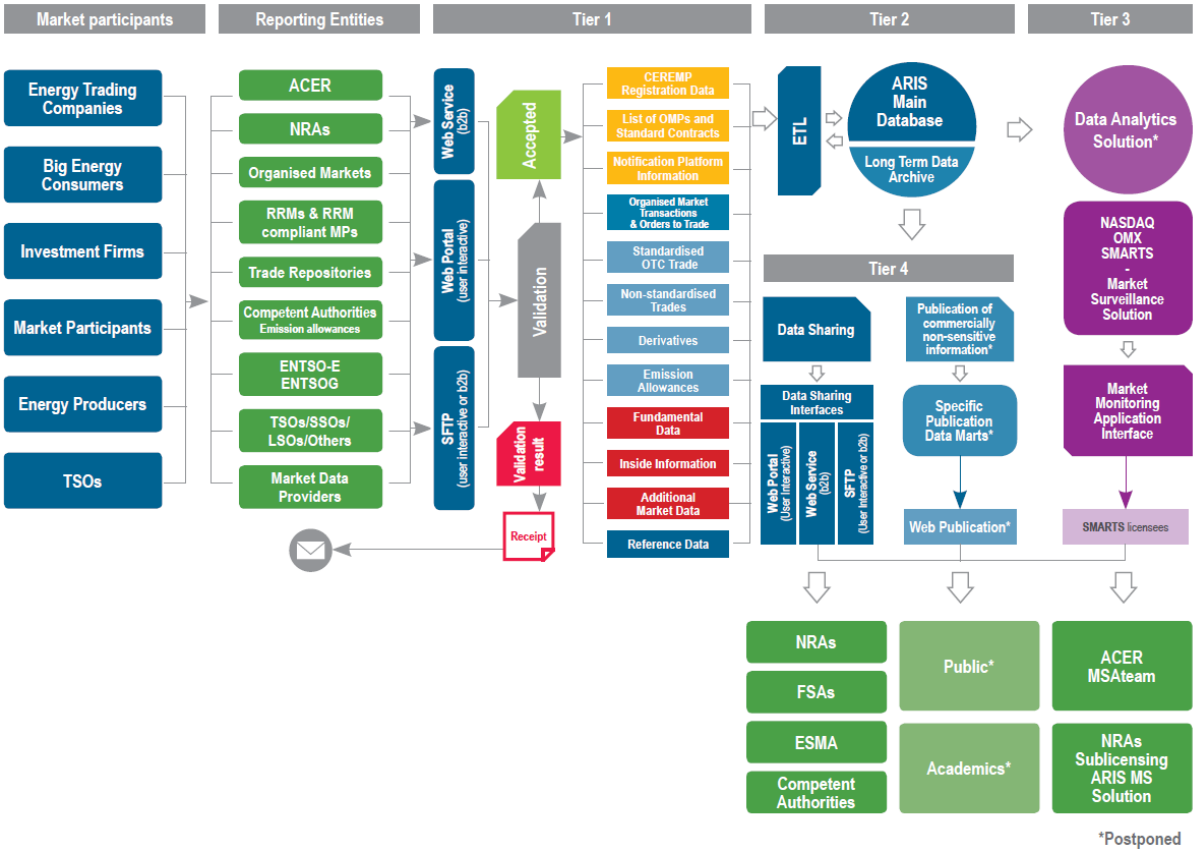
4. Are the minimum technical requirements listed in Annex I.A. fulfilled by the proposed solution?

3.2. Case study for a period of two (2) years

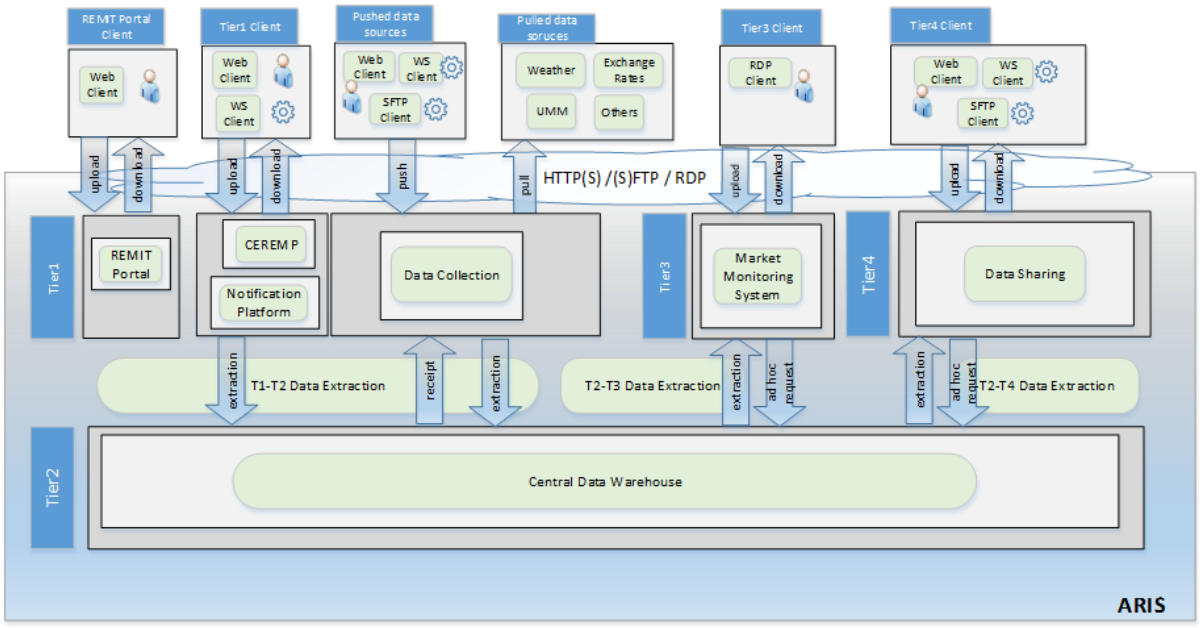
The Agency intends to launch a service request with the aim to cover the need to establish a working hosted system to host a Market Monitoring software platform which should serve twenty-eight (28) National Regulatory Authorities ('NRAs') and the Agency.

The Agency proprietary software will be designed as follows:

Functional view:



Technical view:



The estimations for capacity planning are:

Tier	Computing capacity	RAM capacity	Storage capacity	Storage performance
1	150 GHz	512 GB	5 TB	10.000 IOPS
2	150 GHz	512 GB	10 TB	20.000 IOPS
3	80 GHz	256 GB	10 TB	20.000 IOPS
4	115 GHz	100 GB	5 TB	10.000 IOPS

The list of key software architectural elements[2]:

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Tier 1: Web Server (**Registration, Collaboration, Administration**) web1, web2	2	2	4	100 GB	Apache HTTPD Server	HW LB (sticky session based on SSL Session ID)	Redundancy with 2 Apache servers

[2] If a specific Tier number is not provided for a component it may (but not necessarily has to) be placed in a separate zone (e.g. Tier 5).

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Tier 1: Web and SFTP Server (**Data Collection**) websftp3, websftp4, websftp5, websftp6	4	2	4	150 GB	Apache HTTPD and SFTP Server	HW LB (sticky session based on SSL Session ID only for web apps)	Redundancy with 4 Apache servers
Tier 4: Web and SFTP Server (**Data Sharing**) websftp7, websftp8	2	2	4	150 GB	Apache HTTPD and SFTP Server	HW LB (sticky session based on SSL Session ID only for web apps)	Redundancy with 2 Apache servers
Mail Server mail1, mail2	2	1	1	20 GB	Postfix for outgoing mail (SMTP)		Redundancy with 2 Mail servers
LDAP ldap1, ldap2	2	1	2	20 GB	Open LDAP Server	DNS LB	Redundancy with 2 LDAP servers with Master-Master replication
Authentication Server (**CAS**) cas1, cas2	2	1	4	20 GB	CAS (Central Authentication Service) deployed on Tomcat	HW LB	Redundancy with 2 CAS server in HA configuration
Tier 1: Application Server (**Registration**) app1, app2	2	4	12	100 GB /filestore1 (nfs)	CEREMP, CEREMPWS, NOTIFICATION PLATFORM, etc. deployed on Tomcat	HW LB	Redundancy with 2 application servers
Tier 1:	2	2	12	100 GB	ADMIN apps	HW LB	Web

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
Application Server (**Collaboration, Administration**) app3, app4				/ filestore 1 (nfs)	deployed on Tomcat		applications: redundancy with 2 application servers
Tier 1: Application Server (**Data Collection**) app5, app6, app7, app8	4	2	12	100 GB / /filestore3 (nfs) /data (sshfs)	DCI, DCI-WS, DCI-SCHEDULER apps, etc. deployed on Tomcat	HW LB	Redundancy with 4 application servers
Tier 4: Application Server (**Data Sharing**) app9, app10	2	2	8	100 GB / /filestore4 (nfs) /data (sshfs)	Data sharing web app and ws etc. deployed on Tomcat	HW LB	Redundancy with 2 application servers
Tier 2: Application and SFTP Server (**Data extraction for T3**) app11, app12	2	2	8	100 GB / / filestore 4 (nfs)	Data extraction apps deployed on Tomcat and and sftp deamon	HW LB	Redundancy with 2 application servers
Log Management System app13, app14	2	2	4	20 GB / /filestore2 (nfs)	Log apps deployed on Tomcat	HW LB	Redundancy with 2 application servers
File Server(1) nfs1, nfs2	2	2	2	20 GB / /filestore1 (250 GB) /filestore2 (500 GB)	NFS Server		Active/Passive Heart beat configuration
File Server(2)	2	2	2	20 GB	NFS Server		Active/Passive Heart beat

System / Service	N° Server	N° Vcores / server	RAM (GB) / server	Storage	Software requirements	Load Balancing	Application HA
nfs3, nfs4				/filestore3 (5 TB) /filestore4 (5 TB)			configuration
Terminal Servers	2	8	32	/ Windows O.S. (20GB)	Terminal Server	HW LB	Redundancy with 2 servers
Tier 3: Market Monitoring server	2	8	64	100 GB / Data (2TB)			Fail back server at the secondary site
Tier 2 Database Server (physical)	2	16	128	100 GB Data (2TB)	Oracle 12c R1 DBMS		Oracle RAC

The following additional requirements apply and must be present in the proposed solution:

- F6: 2 x 100 Mbps connection to the internet;
- F9: 1 x 1 Gbps connection between primary and secondary site;
- F11: 1 x 100 Mbps connection to the Agency;
- K1: 16 public IP addresses;
- K2: 3 domain names (.eu);
- K3: 16 DNS entries;
- I6: 1000 digital certificates from EU accredited CA;
- licensing (H) should be fully covered for OS and Hypervisors provided. No other licenses have to be included in the case study;
- a total of 1,200 man-days for the provision of services measured in man-days (G, I2 – I3, J2 – J4, L). For the purpose of this case study the total number of man-days should be evenly split between profiles (A, B and C) and for each profile 100 man-days should be provided on-site;
- a total of 2,000 requests to the service desk (J1).

For the purpose of this case study the tenderers are also required to consider how they would respond to the Agency's request to co-locate the following equipment without replicating to secondary site:

- C: 1 rack;
- E1: 4 standalone servers for co-location;
- E2: 1 storage controller for co-location;
- E3: 1 network connectivity device – switch for co-location;
- E4: 1 network security device – firewall for co-location;

- E5: 1 backup device for co-location.
- F2: 1 x 100 Mbps connection to Agency's premises
- F4: 1 x 10 Mbps connection to internet

The case study should provide the answers to the following questions:

5. How the infrastructure could be set up and managed?

6. Which type of IT experts should be included to set the system up and run it for a period of two (2) years?

7. How the security-related services (I1 – I7), licensing model (H) and support services (J1 – J4) and software related services (G) will be provided?

8. Are the minimum technical requirements listed in Annex I.A. fulfilled by the proposed solution?

3.3. Security applicable to points 3.1 and 3.2 above

The case study shall detail out the tenderer's proposal for a security infrastructure which must be reflected in the proposal for the case study. The proposed security infrastructure must contain security devices including firewalls, proxies, Intrusion Detection Systems, Anti Virus, etc.

3.4. Connectivity constraints applicable to points 3.1 and 3.2 above

Connectivity must be assured to the system end-users with an internet secure communication channel. The Agency will provide SSL certificates for the web server. All the other layers of the hardware platform should be secured as much as possible and in a transparent way. Peaks of 2.000 concurrent sessions may take place and the Agency's software is able to support such peaks. All components provided in the case study (hardware and each piece of equipment) must be able to assure the same level of performance.

The system will need to provide each of the 28 NRAs and the Agency with a secure communication channel in order to process all the requests forwarded from/to the Agency and from/to the NRAs. Easy and manageable solutions based on VPN appliances are the preferred Agency's option. In order to reduce costs, the Agency will rely on existing internet connectivity at the NRAs side, and will allow the adoption of a central appliance at the hosting site. This need needs to be reflected in the proposed infrastructure.

A secure connection channel with the hosting provider shall be provided to the Agency. The secure connection channel shall be able to reach the hosted hardware and to provide any operation, including remote hardware reset of each provided component. A dedicated connection is the Agency's preferred option. The proposal for the case study shall include a communication line together with all the equipment to secure it.

4. Services to be provided by the tenderer applicable to points 3.1 and 3.2 above

- Installation and management of a fully working platform fully implementing the topology and the hardware configuration.
- Installation and management of Operating Systems.
- Installation and management of Data Base Systems.
- Installation and management of Application Servers.
- Installation and management of all listed ancillary services.
- All security configurations as proposed.
- Configuration of each connectivity channel.