Terms of Reference (ToR) for the provision of Support Services for the ICT Back-end Infrastructure Systems

Background

The Information and Communications Technology Services (ICT) of the Organization for Security and Cooperation in Europe (OSCE) provides various ICT services on different infrastructure and systems products in the Secretariat (Wallnerstrasse 6, 1010 Vienna, Austria and Hofburg, 1010 Vienna, Austria), OSCE disaster recovery site (Fernkorngasse 10, 1100 Vienna, Austria) and among Executive Structures; list of the OSCE locations (Executive Structure) is available at www.osce.org/where-we-are

The OSCE server and client infrastructure is primarily based on Microsoft products. The installed user base is approximately 4,000 and 200+ servers (physical and virtual) among all OSCE Executive Structures.

1. Service/products covered by the Tender

The OSCE is seeking to establish a Support Service Contract with a qualified Vendor covering the architecture and design, implementation, maintenance and support, training and upgrade of the following services/products:

MicroFocus:

- Access Manager 4.x
- Identity Manager 4.x
- Sentinel 8.x

SuSe:

- SuSe Linux Enterprise Server 11, 12

Microsoft:

- Windows Server 2008 R2 – 2016
- Active Directory
- Kerberos authentication
- DNS
- DHCP
- DFS
- File Server
- Print Server
- PKI

- IIS
- Exchange 2010 – 2016
- Lync 2010
- Skype for Business 2015
- SQL Server 2008 – 2017
- KMS
- SCCM 2012
- SCOM 2012 - 2016
- Remote Desktop Services
- ADFS
- Microsoft 365
- Microsoft Azure
- Windows 7 – 10
- Group Policy Management
- Microsoft Plans and Licensing
- Tenancy administration
- SharePoint 2013 – 2016
- Office 2010 – 2016
- Advanced Threat Analytics
- Network Policy Server
- Identity Manager
- Privileged Access Management
- Rights Management Services

VMWare:

- vSphere 5.5 – 6.7
- vCenter 6, 6.7
- Site Recovery Manager 6.x, 8.x
- vRealize Operations Manager 6.x
- NSX 6.x
- AirWatch 9.x and mobile device troubleshooting (iOS and Android) – (optional)

RSA:

- ACE 8.x

McAfee:

- ePolicy Orchestrator 5.x
- McAfee Agent 5.x
- McAfee Endpoint Protection 10.x
- Virusscan Enterprise 8.x
- McAfee protection for SharePoint 3.x

Kaspersky:

- Kaspersky Security 9.x for Exchange
- Kaspersky EndPoint Security 11.x
- Kaspersky Security Center 10.x

Baramundi:

Baramundi Management Suite 2018 – (optional)

In addition to the services above, the OSCE ICT, require assistance in the following areas:

- Operational backup for the OSCE platform team;
- Operational backup for the OSCE client management team;
- Backup for OSCE platform team in case of disaster recovery;
- PowerShell script development;
- Linux troubleshooting;
- Network troubleshooting (e.g., HPE, Cisco, Checkpoint, etc.).

The following backend enterprise products are in use with above listed services/products, thus the Bidders shall have experience with this architecture and those products mix:

- Data Protector 9.x, 10.x ;
- HPE 3PAR ;
- HPE Proliant Servers G7 and higher.

The above-mentioned product versions are the current ones (at the time of publishing of this tender); the appointed Contractor shall provide support for future versions for the duration of the Contract as well.

2. Objectives

The objective of this tender is to enter into a 5-year Contract for the provision of support services covering Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA products to the OSCE Secretariat located in Vienna, Austria as well as Executive Structures located outside of Austria. Consultants' travel will be arranged at the OSCE daily subsistence allowance (DSA) rates and expenses. The provisioning of the support services shall be based on pre-paid pool hours (in blocks of 25, 50, 100, 250, 500 or 1000 hours), or based on defined projects and with specific Purchase Orders. In any case, the Contractor will be requested to provide an estimate of the required hours per project or support case prior to provisioning the service.

Pre-paid pool hours must not become invalid after one calendar year after purchase but be carried over until the end of Contract.

Objective I: To provide the OSCE with specific technical expertise/consultancy for the application and efficient use of Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA software products, including advice and technical assistance on setup, configuration, maintenance, security as well as new updates and upgrades of these products. The appointed Contractor shall provide technical expertise advice to assist the OSCE decision making on optimum operation and maintenance of referenced software. The Contractor shall advise the ICT in market typical consulting sessions, on best business practice for the utilization of the ICT infrastructure.

Objective II: To provide ad-hoc remote and on-site troubleshoot and incident resolution capacities for the maintenance of an efficient operation of Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA products as a “second level escalation services”. In case the Contractor is not able to resolve the issues, the Contractor shall open service requests with the respective Vendor(s) at no extra cost for the OSCE.

Objective III: Knowledge Transfer and update OSCE staff in the latest technology applications of Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA products (knowledge transfer) in the style of yearly vendor conference events and to provide access to manufacturer product roadmaps to plan investments.

3. Pre-requisite Qualifications

The Bidder, and subsequently the appointed Contractor, shall comply at all times during the term of the contract with the following minimum qualifications and certifications:

3.1. The Bidder shall be at least certified:

- Microsoft Gold Competence Partner;
- Micro Focus Premier Partner;
- VMWare Enterprise Partner;
- SuSe Registered Partner;
- Solution Seller (optional, only if Baramundi support is offered);
- Kaspersky Registered Partner

Any downgrade of the partner status must be reported to the OSCE Procurement and Contracting Unit (PCU) and the OSCE technical contact person at the latest on the end of the month in which change took place.

3.2. At least four members of the Contractor's Key Personnel assigned to perform the Services for the OSCE shall be under the regular employment of the Contractor. Any such member of the Contractor’s Key Personnel shall hold valid certificates of the following list in Table No.1 at any time during their assignment to the OSCE and minimum 3 years of professional experience in the products utilized by the OSCE. If external Consultants are proposed to cover certain fields of experience, these must be clearly marked in the Bidder’s proposal.

Tab. No. 1 – Certification Requirements

No.	Certification Status
1.	VMWare Certified Professional – Data Centre Virtualization
2.	Microsoft Certified Solution Associate: Windows Server 2016
3.	Microsoft Certified Solution Expert: Productivity (Exchange 2016)
4.	Microsoft Certified Solutions Associate: Windows 10
5.	Microsoft Certified Solution Associate: Office 365
6.	vmWare AirWatch certification level Enterprise Mobility Associate (optional, only if AirWatch support is offered)

Copies/screenshots of valid certificates must be included in the proposal.

3.3. The Bidder shall have proven experience (in the form of project references, preferably in the public sector/international organizations) in providing similar support/consultancy services to an international organisation, or business with an international presence, comparable to the OSCE.

3.4. The appointed Contractor shall be willing and capable to accept short temporary assignments of its personnel to any OSCE location, including the OSCE field operations, as required by the OSCE.

3.5. All communication, written or verbal, shall be conducted in English. The designated OSCE account manager as well as the Contractor's assigned staff shall demonstrate fluency in English.

3.6. The Contractor's key personnel need to be announced and registered by name. Changes in the key personnel shall be announced immediately to the OSCE.

3.7. The service delivery needs to be provisioned by the Contractor's staff. Subcontractors may only be used after prior agreement with the OSCE.

4. The OSCE's Requirements

The Contractor shall comply with following requirements:

4.1. The Contractor's key personnel must be familiar and up to date with all ICT systems deployed at the OSCE in respect to Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA applications. In order to achieve that, familiarization with OSCE specific systems shall be performed during an (estimated) 5 working days' initial session on-site in the OSCE Secretariat in Vienna, Austria at no additional cost to the OSCE.

4.2. The Contractor shall plan and propose to the OSCE the scope and the methodology of knowledge transfer to the OSCE staff in accordance with the scope of Services described herein and in particular under requirement 2.5.6.

5. Scope of Services

The Contractor shall provide the following scope of services. For this purpose, the Contractor shall be prepared to conduct on-site visits to any OSCE Executive Structure, shall provide telephone or remote support and shall attend information exchange meetings in Vienna, Austria.

5.1. Reports

The Contractor shall provide monthly attendance records in electronic form to document any Services performed on-site, by telephone or by remote assistance. Each report shall include, but not be limited to information regarding the date, the time and the duration of performance, the name(s) of the member(s) of the Contractor's personnel that has/have performed the Services, the OSCE location of performance, the ICT request originator and the number and date of the applicable Purchase Order if any. Such reports shall be done electronically and in such detail as necessary to allow tracking of the hours actually performed by the Contractor's personnel. The OSCE shall have access to a web based portal for pool hours status and services rendered.

Upon request from the OSCE ICT Program Manager, the Contractor shall provide reports, such as testing of hardware and/or software elements and, subject to mutual agreement between the Key Personnel and the OSCE ICT Program Manager, any other report related to the Contractor's performance of in scope Services on a case-by-case basis. Such report shall contain, but not be limited to, a product overview, a reference to the infrastructure category, a description of environment utilized, functions and specifications of the product tested.

The Contractor shall provide quarterly service performance reports, which demonstrate the compliance with the required service levels. The service performance reports shall be reviewed in quarterly service meetings in person at the OSCE Secretariat in Vienna, Austria. Upon request from the OSCE ICT Program Manager, additional meetings may be scheduled with the Contractor.

The Contractor shall provide a secure web portal for monitoring service requests as well as pool hour status. The web portal shall be multi-tenant capable (units see only their service requests and pool hours).

Objective I – Provision of Specific Technical Expertise – Consulting

5.2. Consulting

Consulting services shall be provided to the OSCE in the form of a project or work package (WP). The Contractor shall be tasked to submit specific deliverables on specified deadlines mentioned in the project or WP, which will be mutually agreed and confirmed in advance by the OSCE and the Contractor. The project or WP may focus on the introduction of a new service, a problem management case, or infrastructure architectural design.

Before selecting a new product, or strategy to implement a certain product from Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA or a product requiring their interoperability, the Contractor shall, upon request of the OSCE, conduct and provide the OSCE with a product assessment and risk analysis report, enabling the OSCE to make an informed decision. The specific terms and conditions, including project deliverables, OSCE acceptance criteria and time sheets, shall be mutually agreed upon between the Parties and shall be documented accordingly. Upon request of the OSCE and as part of the deliverables, the Contractor shall provide a proof of concept, approved by Micro Focus EMEA, Microsoft EMEA, HP EMEA, VMWare EMEA, McAfee EMEA, Baramundi EMEA, Kaspersky EMEA or RSA EMEA.

Please describe the methodology and work plan for provision of these services.

5.3. Software Testing

The Contractor shall provide to the OSCE Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA “beta software” when it becomes available. This test software shall not be used for production environments unless agreed upon by Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi, RSA and the Contractor. In any event, the beta software shall be used by the OSCE for trial purposes only and at no additional cost to the OSCE.

Upon request from the OSCE, the Contractor shall also conduct product tests of specific software products as defined and required by the OSCE, which are not part of the Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA product range. In the event that the relevant software manufacturer does not provide trial, time-bomb or other test software free of charge, the Contractor shall provide such software product to the OSCE on an “at cost” basis.

Please describe the methodology and work plan for provision of these services.

5.4. ICT Staff Replacement

Upon request from the OSCE, the Contractor shall provide on-site client or second level support services to the OSCE ICT primarily at the OSCE Secretariat in Vienna, Austria (and in any other location of the OSCE as required). Such requirements may in particular occur, for example:

a) during general leave periods of OSCE staff, e.g. during summer months, or
b) during resource-intense ICT project implementations;
c) during unforeseen availability of OSCE staff, e.g. sick leave, emergencies etc.

These support services shall include day-to-day routine checks of in scope services, service availability, performance checks, user account management, access right administration and urgent software upgrades, change requests to the infrastructure and roll-out of patches in liaison with OSCE ICT and Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA. The OSCE shall inform the supplier of such requirements 2 weeks in advance for case (a) and (b) and 4 days in advance for case (c). Case (c) shall be supplied on a best-effort basis.

The estimated annual quantity for the ICT staff replacement for will be 20 days per annum.

Objective II – Provision of Incident Resolution Services

5.5. The Contractor shall provide incident analysis and resolution services in accordance with the following provisions:

- The Contractor shall receive requests for support by OSCE staff members, as determined by the OSCE, via telephone (support hotline) or email in English;
- The Contractor shall acknowledge the new request within 3 hours after receipt of the request for support from the OSCE;

- The Contractor shall provide support within the following working hours:

  - 5 days a week (Monday to Friday) / 08:00 till 18:00 Vienna, Austria local time, all priorities
  - Saturday, Sunday, official OSCE holidays (OH) / 08:00 till 20:00 Vienna, Austria local time, priority Red
  - OSCE ICT Maintenance Windows (MW) / 18:00 till 21:30 Vienna, Austria local time every second and fourth Tuesday of the month, priority Red

- The Contractor shall provide analysis to the reporting issue and workaround/fix within the times specified below:

Tab. No. 2 – Timeframe Requirement (Service Level)

No.	Priority	Impact	Response time, Mon–Fri	Response time, Sat–Sun MW/OH	Resolution time
1.	Yellow	User impact	8 hours	N/A	2nd NBD**/mutual agreement
2.	Orange	Service degradation	6 hours	N/A	NBD
3.	Red	Service unavailable	6 hours	3 hours	6 hours “work through”*

** work through – The Contractor shall work continuously on the blocking problem until a workaround or resolution to the unavailability is found and is technically implemented.*

*** NBD – next business day*

- The Contractor shall be onsite at the OSCE Secretariat or DR site within three (3) business hours in case of “red” priority situations which require on site availability upon request of the OSCE;
- The Contractor’s certified staff needs to be available in emergency situations.

In case there is an urgent operational requirement, qualified key members from the Contractor shall provide support primarily on-site at the OSCE Secretariat in Vienna, Austria but also be ready to conduct on-site visits to any OSCE Mission, Institution and Field Operation if required.

In the event that the incident cannot be resolved within the agreed resolution time for evident technical reasons (i.e. manufacturer knowledge base has confirmed a software bug), the Key Personnel of the Contractor and the OSCE ICT Program Manager shall mutually agree on such additional time period to satisfactorily resolve such incident.

Due consideration shall be given to the interests of the OSCE and the provision of uninterrupted ICT services to the Organization.

The Contractor shall provide support for Red priority incidents during the OSCE ICT maintenance windows, as per defined schedule that will be provided by ICT to the Contractor at the beginning of each calendar year (subject to changes). The Contractor shall focus on specific on-site escalation and troubleshooting services in respect to unexpected or unforeseen incidents occurring during maintenance work conducted by ICT. The Contractor shall make available resources to cover such maintenance windows remote or on-site. The on-site support for the maintenance windows shall be provided primarily in the Secretariat in Vienna, Austria.

The Contractor shall be authorized to create service requests/support calls on behalf of the OSCE and upon the OSCE's request for all used products.

Objective III – Knowledge Transfer

5.6. The Contractor shall provide knowledge transfer in English to the OSCE ICT staff to update their knowledge and application skills of the relevant scope and performance of the Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA product family. An exact schedule for conducting the knowledge transfers and the topics to be covered shall be mutually agreed upon as between the Contractor and the ICT. The knowledge transfer may be delivered in the style of yearly vendors' conference events.

The OSCE shall retain the right to change the knowledge transfer sessions, at any time by adding or deleting requirements, provided they are within the defined service portfolio. The cost of each knowledge transfer session shall be quoted on the basis of a fixed daily rate and other costs stipulated.

The estimated annual quantity will be one 5-days knowledge transfer session per annum in Vienna, Austria. Such knowledge transfer sessions may be requested also in an OSCE Executive Structure.

The knowledge transfer shall include an update on the latest developments within and technological knowledge of the Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA product family (details and scope similar to the sessions scheduled at the annual Vendor Conference event) and shall be provided by a member of the supplier's Key Personnel to selected ICT users within the OSCE. Facilities and equipment required for the knowledge transfer shall be provided by the OSCE.

5.7. In addition, one member of the Contractor's Key Personnel shall provide Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA-related knowledge updates to ICT staff in quarterly sequences, i.e. brief the OSCE ICT staff about latest developments, bugs, usability issues and other topics. The level of detail of such briefings shall be targeted to match and improve competence of senior ICT administrative assistants, highly skilled in the Microsoft, Micro Focus, VMWare, SuSe, McAfee, Kaspersky, Baramundi (optional) and RSA environment.

Appendix I – Format of Curriculum Vitae (CV) for Proposed Professional Staff

First Name:
Last Name:
Date of birth:
Functional title:
Company name:
Years with the Company:

Detailed tasks assigned:

Key Qualifications:

Give an outline of staff member's experience and training most pertinent to tasks on assignment. Describe degree of responsibility held by staff member on relevant previous assignments and give dates and locations. Use about half a page

Education:

Summarize college/university and other specialized education of staff member, giving names of schools, dates attended, and degrees obtained. Use about one quarter of a page

Employment Record:

Starting with present position, list in reverse order every employment held. List all positions held by staff member since graduation, giving dates, names of employing organizations, titles of positions held, and locations of assignments. For experience in last ten years, also give types of activities performed and suppliers' references, where appropriate. Use about two pages

Certifications:

Include the required certification

Languages:

For each language indicate proficiency: excellent, good, fair, or poor in speaking, reading, and writing