UNDP's Response to Proposers' Question
RFP/UNDP/OIST/004/2015
RFP for the provision of Cloud Security Gateway – Round 1

1. Question is on the financial proposal in section 7, if we use a reseller will the partner have to respond to the RFP as well?

Although the proposer can work with partner in delivering the required service (the proposal should clearly explain how the entities would interact), there should be one designated lead entity who will be submitting the proposal and signing the contract if awarded.

2. In section 8 where it states professional services/contractors. Is there anything to fill out or are these expected guidelines to have in place prior to performing services?

No. Section 8 is a template of the contract that will be issued to the winning bidder.

3. Will you please clarify if we are we filling in items outside of sections 4-7? For example: the RFP states section 15 (technical proposal and point of contact) and 15.1 (expertise of firm organization). Are these points of reference for the other sections or will the bidder be responding to these items too?

Please use the Sections 4-7 as a template in preparing the proposal. But make sure that the information provided would be able to respond to the requirement (Terms of Reference) as well as the evaluation criteria stated on page 24-27 of the RFP. Also, please read Section 2 (Instructions to Proposer) on how to submit the bid.

4. The RFP requests a proposal for unlimited users with unlimited applications. Would it be acceptable to provide a response with a proposal for 30,000-50,000 users with unlimited applications?
We need to have unlimited number of users with unlimited applications. At present we have approximately 40,000 unique users of all of our cloud services. This could grow in the future.

5. Would you please send me another copy of the RFP. I am unable to edit the current document which makes it difficult to parse out certain sections to appropriate individuals in my organization.
Please find attached.

6. **Is the gateway intended for current services only or for future services as well?**
Cloud Gateway is intended for all future cloud services as well. That's why there is a requirement for unlimited number of protected applications

7. Should it be adaptable for new services? How easy adaptable (pls. specify person days UNDP is prepared to spent internally for each new service added)
Yes, solution should be flexible enough to adopt new cloud services. UNDP could not estimate the level of how easy it should be.

8. Which technologies apart from the already disclosed are used to provide the cloud services in question? E.g. AWS etc.
At this point, UNDP uses only technologies mentioned in the RFP. However, solution should be Cloud Service Provider agnostic as much as possible to facilitate integration with future possible Cloud and IaaS providers.

9**. Are the actual applications on the Azure Platform or other IaaS platforms in Scope?**
Yes, UNDP is migrating in-house hosting to Azure and expects all Azure infrastructure to be in scope of the Cloud Gateway in the future.

10. Which level of function/action do you want to be monitored for anomaly behavior.
The primary action is login/authorization activity but solution should be able to monitor other actions on different platforms (O365, etc.). As outlined in the RFP, the more granular and diverse the monitored actions, the better.

11. Are there means to identify those actions, which can be disclosed? i.e. logfiles / APIs etc.
Actions on UNDP ERP could be identified through specific URLs being accessed. Actions on platforms should be identified through APIs exposed by specific Cloud Service Provider (e.g. O365 + ADFS).

12. Is the identification of the actions supposed to be on the gateway only, or can agents be deployed on the cloud services?
It is preferred to avoid the agents being deployed or at least minimize deployment only to a handful of authentication servers (e.g. ADFS).

13. **Do the security profiles already exist?**
Profiles mentioned in RFP are are related to user behavior (logins from specific places, browsers, etc). Policy profiles/roles do exist for actions in UNDP RFP and could be converted to segregation of duty alerts to be generated by the Gateway.

14. How many concurrent users will use the service?
UNDP expects at least 20,000 concurrent users.

15. What volume in terms of network traffic is the gateway expected to handle (Gbit/sec, concurrent IP connections)
UNDP could only estimate concurrent users (see answer #14)

16. Are there latency requirements, i.e. how much additional time can be added to the usual latency of the services
UNDP could tolerate an additional one second delay introduced by the Cloud Gateway solution. Obviously, shorter the delay time the better it is.

17. Are there operational requirements, response time requirements, time to fix , availability etc.
All these are part of the SLA to be negotiated with the perspective RFP winner as part of the contract negotiations.

18. Are there requirements in terms of how encrypted traffic can be decrypted on the gateway?
Cloud Security Gateway solution is envisioned to be integrated into ADFS and act as a substitution or additional login page (2FA) with its own set of HTTPs certificates/key. UNDP could provide HTTPs key for systems under UNDP's control (e.g. ERP). Obviously, third-party cloud services like O365 would require interception/termination of HTTPs traffic on the solution, as no secret HTTPs keys are available to customers of these services.

19. Which kinds of encrypted traffic will be seen?
Mostly TLS with strong ciphers (e.g AES-128) and Perfect Forward Secrecy key exchange (e.g. Diffie–Hellman)

20. Which Protocols are expected: there will be http and HTTPs obviously. Anything else, any binary formats on top of those?
No binary formats, only HTTPs is expected.

21. This next question is on the size of our files exceeding the 5MB threshold:

Based on the submission requirements from UN, we will not be able to provide a financial statement in PDF smaller than 5MB via email. Will you please advise on an acceptable alternate method for complying with this request?

You can split it and send it in several emails.